

Ira M. Siegel, Cal. State Bar No. 78142
email address: irasiegel@earthlink.net
LAW OFFICES OF IRA M. SIEGEL
433 N. Camden Drive, Suite 970
Beverly Hills, California 90210-4426
Tel: 310-435-7656
Fax: 310-657-2187

Attorney for On The Cheap, LLC DBA Tru Filth, LLC

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

On The Cheap, LLC DBA Tru Filth, LLC, a
California corporation,

Plaintiff,

v.

DOES 1-5011,

Defendants.

CASE NO. CV 10-04472 BZ

**PLAINTIFF'S RESPONSE TO ORDER
TO SHOW CAUSE**

JUDGE: BERNARD ZIMMERMAN,
United States Magistrate Judge

Date: August 24, 2011
Time: 10:00 a.m.
Courtroom: C-15th Floor

TABLE OF CONTENTS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

TABLE OF CASES

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

I. INTRODUCTION

On June 24, 2011, the Court issued an Order to Show Cause (Doc. #37).

The Court ordered as follows:

IT IS HEREBY ORDERED that by July 13, 2011, plaintiff shall show cause in writing why this case should not be dismissed as to all Doe defendants but Doe 1 for misjoinder of 21 parties and improper venue. See Diabolic Video Productions, Inc. v. Does 1-2099, 10-CV-05865-PSG, Docket No. 16 (N.D. Cal. 2011); Lightspeed v. Does 1-1000, 2011 U.S. Dist. LEXIS 35392 24 (N.D. Ill. 2011).

II. BACKGROUND FACTS—PLAINTIFF NEEDS THE ASSISTANCE OF COURTS TO ENFORCE ITS COPYRIGHTS AGAINST MASS COPYRIGHT INFRINGEMENT

Much of the following is already familiar to the Court.

Plaintiff is a motion picture production company. The work at issue in this case (the "Work") is titled "Danielle Staub Raw" and is registered in the United States Copyright Office: Registration Number PAu 3-489-521. The Work and the copyright therein are owned by Plaintiff. First Amended Complaint, par. 7 and 8. Declaration of Jon Nicolini filed June 8, 2011 (Doc. #30), par. 10 and 13.

The Court is asked to note that this motion picture, while it is intended for the audience seeking "adult erotic movies," gained fame among general audiences because its star, Daniel Staub, was one of the cast of the Bravo cable television channel series "Real Housewives of" See, e.g., the article titled "Did 'Real Housewife' Danielle Staub Leak Her Own Sex Tape?" here:

<http://www.foxnews.com/entertainment/2010/06/10/did-real-housewife-danielle-staub-leak-sex-tape/>

//

//

//

1 This case is a copyright infringement case. It involves motion picture mass piracy of the
 2 kind that has been plaguing the country as advances in technology have made infringements
 3 almost effortless to accomplish at the same time that identifying the infringers has become more
 4 difficult. This mass piracy is conducted by numerous people participating in a "swarm" of
 5 infringers who use the Internet to illegally copy and distribute motion pictures.¹

6 Former United States Senator Chris Dodd, in his inaugural speech as the new president of
 7 the Motion Picture Association of America, on March 29, 2011, stated,

8 "Let's begin with perhaps the single biggest threat we face as an industry:
 9 movie theft. * * *

10 "I am deeply concerned that too many people see movie theft as a
 11 victimless crime. After all, how much economic damage could there be to some
 12 rich studio executive or Hollywood star if a movie is stolen or someone watches a
 13 film that was stolen? It is critical that we aggressively educate people to
 14 understand that movie theft is not just a Hollywood problem. It is an American
 15 problem.

16 "Nearly 2.5 million people work in our film industry. The success of the
 17 movie and TV business doesn't just benefit the names on theater marquee. It also
 18 affects all the names in the closing credits and so many more - middle class folks,
 19 working hard behind the scenes to provide for their families, saving for college
 20 and retirement. And since movies and TV shows are now being made in all 50
 21 states, Puerto Rico and the District of Columbia, movie theft harms middle class
 22 families and small businesses all across the country.

23 "Those who steal movies and TV shows, or who knowingly support those
 24 who do, don't see the faces of the camera assistant, seamstresses, electricians,
 25 construction workers, drivers, and small business owners and their employees
 26 who are among the thousands essential to movie making."

27 See, e.g., the web page at,

28 <http://www.boxofficemagazine.com/news/2011-03-29-new-mpaa-chief-senator-chris-dodd-delivers-inaugural-state-of-the-industry-speech>

that is attached hereto as Exhibit 5.

¹ "Swarm" thievery enabled by the Internet is, unfortunately, not limited to copyright infringement. Cases of "swarm" or "flash mob" shoplifting are now arising. See the reports at the following web pages about swarm shoplifting events in Washington, D.C., Las Vegas, NV, and St. Paul, MN:

http://www.myfoxdc.com/dpp/news/dc/video-mob-of-teens-rob-dupont-circle-store-042711?utm_medium=twitter&utm_source=twitterfeed

http://www.cbsnews.com/8301-504083_162-20060576-504083.html

<http://www.myfoxtwincities.com/dpp/news/minnesota/st.-paul-stores-suffer-'mob-thefts'-feb-22-2011>

The Court is asked to take notice that the theory of at least some participants in swarm thievery, by shoplifting or by copyright infringement, is that an aggrieved party may be so overwhelmed by the number of people involved and the time, effort and expense required to catch any offender, that few, if any, will be caught, and if any are, it may be a long time before that occurs.

1 In written responses to a series of questions submitted by Variety magazine that were
2 published on April 13, 2011, Vice President Joe Biden stated,

3 "Look, piracy is outright theft. People are out there blatantly stealing from
4 Americans -- stealing their ideas and robbing us of America's creative energies.
5 There's no reason why we should treat intellectual property any different than
6 tangible property.
7 ***

8 "The fact is, media companies have already taken significant steps to
9 adapt their business models to keep up with changes in how we watch movies
10 and listen to music. Content is being offered to consumers in a variety of
11 different ways that make it easy and cost-effective for people to access legal
12 material. Anyone who does not understand this should simply talk with one of
13 my grandkids."

14 The Variety article can be seen here,

15 <http://www.variety.com/article/VR1118035369>

16 and is attached hereto as Exhibit 6.

17 Please note that Vice President Biden was talking about everyday people committing
18 piracy. One of the biggest, if not the biggest, means by which copyright "pirates" engage in theft
19 of motion pictures is through peer-to-peer networks on the Internet. See, the January 2011
20 Report by Envisional Ltd. that was commissioned by NBC Universal to analyze bandwidth usage
21 across the internet with the specific aim of assessing how much of that usage infringed upon
22 copyright.

23 The Envisional Report can be seen here,

24 http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf

25 and is attached hereto as Exhibit 8.

26 Key findings set out in the Envisional Report include these:

- 27 • Across all areas of the global internet, 23.76% of traffic was estimated to be
28 infringing. This excludes all pornography, the infringing status of which can
be difficult to discern.
- The level of infringing traffic varied between internet venues and was highest
in those areas of the internet commonly used for the distribution of pirated
material.
- BitTorrent traffic is estimated to account for 17.9% of all internet traffic.
Nearly two-thirds of this traffic is estimated to be non-pornographic
copyrighted content shared illegitimately such as films, television episodes,
music, and computer games and software (63.7% of all bittorrent traffic or
11.4% of all internet traffic).

* * *

- In the United States, 17.53% of Internet traffic was estimated to be infringing. This excludes all pornography. A breakdown of internet usage yields the following results:
- Peer to peer networks were 20.0% of all internet traffic with bittorrent responsible for 14.3%. The transfer of infringing content located on these networks comprised 13.8% of all internet traffic.
- As would be expected of copyright pirates, they do not come forward and openly identify themselves, and many behave with the implicit understanding that catching them would be difficult.

* * *

BitTorrent

- BitTorrent is the most used file sharing protocol worldwide with over 8m simultaneous users and 100m regular users worldwide.
- Over 2.72m torrents managed by the largest bittorrent tracker were examined for this report. Our analysis suggests nearly two-thirds of all content shared on bittorrent is copyrighted and shared illegitimately.
- An in-depth analysis of the most popular 10,000 pieces of content managed by PublicBT found:
 - 63.7% of content managed by PublicBT was non-pornographic content that was copyrighted and shared illegitimately
 - 35.2% was film content – all of which was copyrighted and shared illegitimately
 - 14.5% was television content – all of which was copyrighted and shared illegitimately. Of this, 1.5% of content was Japanese anime and 0.3% was sports content.
 - 6.7% was PC or console games - all of which was copyrighted and shared illegitimately
 - 2.9% was music content – all of which was copyrighted and shared illegitimately
 - 4.2% was software – all of which was copyrighted and shared illegitimately
 - 0.2% was book (text or audio) or comic content – all of which was copyrighted and shared illegitimately
 - 35.8% was pornography, the largest single category. The copyright status of this was more difficult to discern but the majority is believed to be copyrighted and most likely shared illegitimately⁴
 - 0.48% (just 48 files out of 10,000) could not be identified

⁴For the purposes of this report, the copyright status of any pornography identified is ignored, though the piracy of such content is obviously of interest to the adult video industry (reflected in the many legal suits filed against downloaders during 2010).

Envisional Report, pp. 2-5. (Emphasis omitted, some footnotes omitted.)

The Constitution at Article I, Section 8, Clause 8, empowers Congress to provide for an author's exclusive rights to his works. The tool Congress provided to fight all this piracy is the Copyright Act, 17 U.S.C. §§ 101 etc., and copyright owners must themselves, pursuant to the Act, engage the United States District Courts to enforce their rights.

As is clear from the statements of Vice President Biden and former Senator Dodd, movie studios are suffering greatly from the fact that a great many people are willing to thumb their noses at the Constitution and the Congressionally enacted Copyright Act now that they have a way of semi-anonymously pirating works through the Internet. **Copyright owners such as Plaintiff obviously need the assistance of courts, and not judicial obstacles put in the way of copyright enforcement.**

In Call of the Wild Movie, LLC v. Does 1-1,062, (D. DC Case No. 10-CV-0445, decided March 22, 2011)², in an opinion (attached hereto as **Exhibit 2**) relating to three cases with a total of 5583 Doe defendants' being involved, U.S. District Judge Beryl Howell noted as follows at pp. 12-13:

"Given the administrative burden of simply obtaining sufficient identifying information to properly name and serve alleged infringers, it is highly unlikely that the plaintiffs could protect their copyrights in a cost-effective manner. Indeed, Time Warner urges the Court to sever the defendants for this very reason. Time Warner asserts that, if joinder were disallowed, its burden of complying with subpoenas would be diminished because the plaintiffs would not be able to proceed against all of the putative defendants individually."

In that case, ISP Time Warner Cable sought to quash the subpoenas seeking information about the Doe defendants' identities. Three putative defendants whose identities were disclosed, and amici Electronic Frontier Foundation, Public Citizen, American Civil Liberties Union Foundation, and American Civil Liberties Union of the Nation's Capital, unsuccessfully supported Time Warner Cable's motion to quash, challenging, among other things, personal jurisdiction over doe defendants that likely resided outside of the district in which the litigation was pending.

In the instant case, Defendants Does 1-5011, many of whom are likely residents of this judicial district, have, without the consent of Plaintiff, cooperatively acted with each other to distribute among themselves unauthorized copies of the Work. The available evidence indicates that more than 1 out of every 7 of the Defendants' IP addresses is likely physically located in

² Call of the Wild Movie, was favorably cited by United States District Judge Edward M. Chen in MCGIP, LLC v. Does 1-18, Northern District of California Case No. CV 11-1495 EMC (N.D. Cal. June 2, 2011) (Doc. #14). While Judge Chen noted that the case before him did not include 100s or 1000s of Doe defendants, the reasoning used by him would be the same even if that many Doe defendants were included.

1 California, and of those, more than 1 out of every 5 is likely in this judicial district. First
2 Amended Complaint, par. 10 and 11. Nicolini Decl., par. 23.

3 Defendants engaged and continue to engage in infringement of Plaintiff's copyright
4 through online media distribution systems. Nicolini Decl., par. 16 and 22. Users such as
5 Defendants load software onto their computers that allows them to join file-sharing networks,
6 often referred to as "peer to peer" or a "P2P" networks, to locate and transfer files to and from
7 other users. In order to use the software to locate and exchange files, a user connects to the
8 Internet. Nicolini Decl., par. 4-9.

9 Users subscribe to the services of an Internet Service Provider ("ISP"), such as the ISPs
10 listed in **Exhibit A** attached to the First Amended Complaint, to gain access to the Internet.
11 Each time a subscriber accesses the Internet, the ISP provides a unique Internet Protocol ("IP")
12 address to the subscriber. An ISP generally records the times and dates that it assigns each IP
13 address to a subscriber and maintains for a period of time a record of such an assignment in logs
14 maintained by the ISP. In addition, the ISP maintains records which typically include the name,
15 one or more address, one or more telephone numbers, and one or more email addresses of the
16 subscriber. With an IP address and Timestamp, the ISP having control of an IP address can
17 identify and produce the logs and records that include the Defendant's name, address, telephone
18 number, and email address. Currently, subscriber identifying information associated with each
19 IP address/Timestamp combination is known by, and only by, the ISP. Nicolini Decl., par. 18-
20 23.

21 P2P technology relies on the ability to identify the computers to and from which users
22 can search and exchange files. The technology identifies those computers by the IP address from
23 which the computer connects to the Internet. Taking advantage of this technology, Plaintiff's
24 contractor, Copyright Enforcement Group, LLC ("CEG"), inspects file-sharing networks for
25 computers that are distributing at least a substantial portion of a copy of a copyrighted work
26 owned by Plaintiff, and when CEG finds such a computer, CEG records the IP address of the
27 computer and the date and time ("Timestamp") of the recording. In addition, CEG uses available
28 databases to record the name of the ISP having control of the IP address and the state (and often

the city) associated with that IP address. However, because of the partially anonymous nature of the P2P Internet distribution system used by Defendants, the true names, street addresses, telephone numbers and email addresses of Defendants are unknown to Plaintiff at this time. CEG also downloads the available file from a subscriber's computer, and later runs visual observations to confirm whether or not the file is a copy of at least a substantial portion of a copyrighted work of Plaintiff. CEG has confirmed that each of the files obtained from the Defendants that are listed in **Exhibit A** is a copy of a substantial portion of the copyrighted work listed in **Exhibit A**. Nicolini Decl., par. 17-19.

Exhibit A attached to the First Amended Complaint lists on a Defendant-by-Defendant basis (one Defendant per row) the Work, and its copyright registration number, the IP address associated with each Defendant, the identity of the ISP associated with the IP address, a date and time (the Timestamp referred to earlier) that infringement by that Defendant was observed, and the software protocol used by the Defendant. Nicolini Decl., par. 21.

III. MAGISTRATE JUDGE GREWAL'S RECOMMENDATION IN *DIABOLIC VIDEO PRODUCTIONS, INC. V. DOES I-2099*, 10-CV-05865-PSG, DOCKET NO. 16 (N.D. Cal. 2011) IS BASED ON A MISREADING AND/OR MISINTERPRETATION OF CASE LAW

A. PLAINTIFF'S CASE IS NOT FRIVOLOUS AND THE DISCOVERY SOUGHT IS JUSTIFIED

As a prelude to making his erroneous recommendation, Magistrate Judge Grewal cited cases apparently to imply results that actually do not follow.

Magistrate Judge Grewal cited Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999) for this proposition (CV 10-05865 PSG, ECF #16, p 4):

"[p]eople who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discovery their identity."

In neither the Columbia Ins. case and this case, there was and is not indication that the lawsuit is frivolous, and Columbia Ins. ruled that the discovery would be allowed once the court approved the discovery process.

Magistrate Judge Grewal cited Wakefield v. Thompson, 177 F.3d 1160, 1162 (9th Cir. 1999); Gillespie v. Civiletti, 629 F.2d 637, 642 (9th Cir. 1980), and Gomez v. Serv. Employees Int'l Local 87, No. C 10-01888, RS, 2010 WL 4704407, at *3 (N.D. Cal. Nov. 12, 2010), for the proposition that exceptions to the general rule against expedited discovery are disfavored. (CV 10-05865 PSG, ECF #16, p 4.)

None of these cases stand for that proposition. In addition, in both Wakefield and Gillespie the Ninth Circuit reversed the district courts' dismissal of doe defendants in both of those cases and ordered the district court to allow discovery for the purpose of obtaining information about the doe defendants' identities. In Gomez, the court dismissed the does from the case. But, in that case, it was clear that plaintiff's had already named, identified and served the principal defendant and had already had a Rule 26 conference with the principal defendant. Moreover, this court specifically stated in Gomez (emphasis added),

"The use of 'Doe' defendants is disfavored in the Ninth Circuit. See Gillespie v. Civiletti, 629 F.2d 637, 642 (9th Cir. 1980). **Where the identity of alleged defendants cannot be known prior to the filing of a complaint, however, the plaintiff should be given an opportunity through discovery to identify them.** Id."

In the instant case, Plaintiff has to list the defendants as doe defendants and obtain discovery as to their identities.

B. JOINDER OF DEFENDANTS IS APPROPRIATE, AND, EVEN IF IN DOUBT, SHOULD NOT BE A BAR TO THE DISCOVERY SOUGHT AT THIS STAGE OF LITIGATION

Magistrate Judge Grewal correctly noted that Gillespie holds that discovery should be allowed unless it is clear that the discovery would not uncover the identities of the doe defendants, and he correctly noted that the discovery Plaintiff seeks would uncover those identities.

But when it comes to the other factor that Gillespie set forth for denying discovery, Magistrate Judge Grewal made a serious error in ruling that "*as to all but a single Doe, Diabolic's complaint would, and should, be dismissed for misjoinder.*" (CV 10-05865 PSG, ECF #16, p. 5.)

1 Magistrate Judge Grewal reached that conclusion, and made his recommendation in the
 2 concluding section of his Order that the case be dismissed for misjoinder, even though he
 3 acknowledged that Fed.R.Civ.P. 21 expressly forbids dismissing a case for misjoinder.

4 Somewhere in the middle, Magistrate Judge Grewal shifted grounds and relied on the
 5 following from Rule 21, "On motion or on its own, the court may at any time, on just terms, add
 6 or drop a party. The court may also sever any claim against a party." However, Magistrate Judge
 7 Grewal did not indicate any "just terms" for dropping or severing parties. Instead, his severing
 8 parties could lead to substantial obstacles put in front of Plaintiff's enforcing its copyright against
 9 the horde of pirates. And, as noted above, his recommendation regarding "dismissal" is
 10 completely unsupported.

11 Magistrate Judge Grewal returned to his joinder argument, stating

12 *"Here, the complaint alleges that 2,099 different defendants reproduced*
 13 *its copyrighted film on at least forty-nine different days. The complaint further*
 14 *alleges that all 2,099 defendants have acted in cooperation with one another 'by*
 15 *agreeing to provide, and actually providing, on a P2P network, an infringing*
 16 *reproduction of at least substantial portions of Diabolic's copyrighted Motion*
 17 *Picture, in anticipation of the other Defendants doing likewise with respect to that*
 18 *work and/or other works.' Citing Mr. Nicolini's identification of a common hash,*
 19 *or alphanumeric representation, among all Defendants' content files, Diabolic*
 20 *contends that Defendants joined in a common 'swarm,' or upload and download*
 21 *of the copyrighted work, that qualifies as the single transaction or series of*
 22 *closely-related transactions recognized under Rule 20. This court and others,*
 23 *however, have repeatedly held that the mere allegation that defendants have used*
 24 *the same peer-to-peer network to infringe a copyrighted work is insufficient to*
 25 *meet the standards for joinder set forth in Rule 20. Apart from its lone allegation*
 26 *that Defendants all used the same P2P network to reproduce and distribute*
 27 *Diabolic's copyrighted work, Diabolic offers no allegations whatsoever to support*
 28 *its theory of a single or closely-related transactional theory.*

12 *"To be fair, other courts have deferred the question of joinder and*
 13 *severance until after discovery has been authorized and a motion to quash filed.*
 14 *But in each of these cases, the court appears to have accepted the argument that a*
 15 *file-sharing protocol like BitTorrent 'makes every downloader also an uploader of*
 16 *the illegally transferred file(s).' But neither this case law, nor Diabolic, explains*
 17 *how or why the technical architecture of BitTorrent is any different from those of*
 18 *the file-sharing protocols considered in Leface Records, LLC, Interscope*
 19 *Records, BMG Music, or Twentieth Century Fox Film Corp. In each of those*
 20 *cases, the peer-to-peer nature of the protocol was insufficient to justify joinder of*
 21 *dozens of otherwise unrelated defendants in a single action. Here, Diabolic*
 22 *proposes to join not merely dozens, but thousands, of defendants in a single*
 23 *action. While the court is limited in its technical understanding by the ex parte*
 24 *nature of Diabolic's motion, it can take notice of the fact that the protocols at*
 25 *issues in those earlier cases, like the BitTorrent protocol here, were of precisely*
 26 *the same peer-to-peer architecture."*

(CV 10-05865 PSG, ECF #16, p. 6.) (Footnotes omitted. Note, cases cited above and in omitted footnotes are discussed below.)

Here, Magistrate Judge Grewal gives improper weight to Plaintiff's allegations and the explanations in the declaration testimony of Mr. Nicolini, and (in the omitted footnotes), misinterpreted case law. As discussed below, the cases cited by Magistrate Judge Grewal were not tied up in the technology. The plaintiffs in those cases failed to allege that the defendants acted in cooperation with each other.

Plaintiff contends that joinder is appropriate in this case. However, Plaintiff asserts also that the matter of joinder is not appropriately considered a bar to discovery at this stage of litigation.

With respect to joinder, the controlling rule is Fed. R. Civ. P. 20. It states in pertinent part,

Rule 20. Permissive Joinder of Parties

(a) Persons Who May Join or Be Joined.

(2) Defendants.

Persons * * * may be joined in one action as defendants if:

(A) any right to relief is asserted against them jointly, severally, or in the alternative with respect to or arising out of the same transaction, occurrence, or series of transactions or occurrences; and

(B) any question of law or fact common to all defendants will arise in the action.

(3) Extent of Relief.

Neither a plaintiff nor a defendant need be interested in obtaining or defending against all the relief demanded. The court may grant judgment to one or more plaintiffs according to their rights, and against one or more defendants according to their liabilities.

(b) Protective Measures.

The court may issue orders — including an order for separate trials — to protect a party against embarrassment, delay, expense, or other prejudice that arises from including a person against whom the party asserts no claim and who asserts no claim against the party.

"Under the Rules, the impulse is toward entertaining the broadest possible scope of action consistent with fairness to the parties; joinder of claims, parties and remedies is strongly encouraged." United Mine Workers of Am. v. Gibbs, 383 U.S. 715, 724 (1966).

In this case, Plaintiff alleges that all the Doe defendants have engaged in the same transaction, occurrence, or series of transactions or occurrences, namely, that each of the Doe

1 defendants has infringed the same copyrighted work, and that they did so using the same scheme,
 2 namely using a BitTorrent P2P network, in cooperation with each other. Amended Complaint,
 3 par. 10. Plaintiff further alleges that the Doe defendants have cooperated with each other.
 4 Amended Complaint, par. 11. The allegations are supported by the Nicolini Declaration (Doc.
 5 #30). See, for example, par. 22 of the Nicolini Declaration wherein Mr. Nicolini testifies, among
 6 other things,

7 "the hashes associated with the torrent files on the computers having the IP
 8 addresses and time stamps listed in Exhibit A are all identical to each other, that
 9 is, they all have the same hash. This demonstrates that all the Doe defendants
 listed in Exhibit A joined the same swarm. "

10 In addition, according to BitTorrent, Inc. itself, the very purpose of the BitTorrent
 11 protocol is to allow people to **both** download a file and for them to upload what they had
 12 downloaded to others. Nicolini Decl., par. 7.

13 With respect to the duration of a swarm (and concomitantly, the period of time in which
 14 Defendants can participate in cooperative or joint activity) Mr. Nicolini declares in par. 6
 15 (emphasis added),

16 "Persons seeking to download such a work also access the Internet through an
 17 ISP (which may or may not be the same ISP as used by the original seeder)
 18 and seek out the work on a P2P network. With the availability of the seed,
 19 other users, who are referred to as "peers," access the Internet and request the
 20 file (by searching for its title or even searching for the torrent's "hash" -
 21 described below) and engage the original seeder and/or each other in a group,
 22 sometimes referred to as a "swarm," and begin downloading the seed file. In
 23 turn, as each peer receives portions of the seed, most often that peer makes
 24 those portions available to other peers in the swarm. Therefore, each peer in
 25 the swarm is at least copying and is usually distributing, as a follow-on seeder,
 26 copyrighted material at the same time. Of the over 20,000 infringers tracked in
 27 connection with several cases currently pending, at least 95% of the Doe
 28 defendants were uploading (i.e., distributing) illegal copies of our clients'
 motion pictures at the moment indicated by the Timestamp in the respective
 Exhibit A appended to each complaint, which is also true for this case. In P2P
 networks, the infringement may continue even after the original seeder has
 gone completely offline. Any BitTorrent client may be used to join a swarm.
 As more peers join a swarm at any one instant, they obtain the content at even
 greater speeds because of the increasing number of peers simultaneously
 offering the content as seeders themselves for unlawful distribution. As time
 goes on, the size of the swarm varies, yet it may endure for a long period, with
 some swarms enduring for 6 months to well over a year depending on the
 popularity of a particular motion picture. As a result, the original seed file
 becomes unlawfully duplicated multiple times by multiple parties, with a
 potentially exponential increase in the number of illegal copies of any

1 copyrighted work. With respect to any particular swarm, the hash (an
2 alphanumeric representation of a digital file) associated with the copied file's
torrent file remains the same."

3 So, Magistrate Judge Grewal's analysis clearly misses this point, that the swarm, and joint
4 activity may endure for a much longer period of time than the period involved in the instant case.

5 The foregoing allegations also demonstrate that there are questions of law and fact
6 common to all defendants that may arise in this action, including whether or not each defendant
7 infringed the single copyright in suit.

8 At pages 6-13 of her decision in Call of the Wild, Judge Howell discussed in detail why
9 joinder, particularly at this stage of litigation, is proper in cases such as the instant case. Of
10 particular interest is this observation by Judge Howell at pages 12-13 that explain that
11 consideration of joinder (or severance) at this stage of litigation is inappropriate and could result
12 in plaintiffs' being unable to protect their copyrights in a cost-effective manner (emphasis
13 added):

14 "The plaintiffs, by contrast, are currently obtaining identifying information
15 from ISPs so that they can properly name and serve the defendants. If the Court
16 were to consider severance at this juncture, plaintiffs would face significant
17 obstacles in their efforts to protect their copyrights from illegal file-sharers and
18 this would only needlessly delay their cases. The plaintiffs would be forced to file
19 5,583 separate lawsuits, in which they would then move to issue separate
20 subpoenas to ISPs for each defendant's identifying information. Plaintiffs would
21 additionally be forced to pay the Court separate filing fees in each of these cases,
22 which would further limit their ability to protect their legal rights. This would
23 certainly not be in the 'interests of convenience and judicial economy,' or 'secure a
24 just, speedy, and inexpensive determination of the action.' *Lane*, 2007 WL
25 2007493, at *7 (declining to sever defendants where 'parties joined for the time
26 being promotes more efficient case management and discovery' and no party
27 prejudiced by joinder).

28 **"Given the administrative burden of simply obtaining sufficient
identifying information to properly name and serve alleged infringers, it is
highly unlikely that the plaintiffs could protect their copyrights in a cost-
effective manner. Indeed, Time Warner urges the Court to sever the
defendants for this very reason. Time Warner asserts that, if joinder were
disallowed, its burden of complying with subpoenas would be diminished
because the plaintiffs would not be able to proceed against all of the putative
defendants individually. See Transcript of Mot. Hearing, 14-16, Call of the Wild
Movie LLC v. Does 1-1,063, No. 10-cv-455 (Mar. 1, 2011).**

"At this procedural juncture, the plaintiffs have met the requirements of
permissive joinder under Rule 20(a)(2). The putative defendants are not prejudiced
but likely benefited by joinder, and severance would debilitate the plaintiffs'
efforts to protect their copyrighted materials and seek redress from the putative
defendants who have allegedly engaged in infringing activity. Courts are instructed
to "entertain[] the broadest possible scope of action consistent with fairness to the

parties.'" *Lane*, 2007 WL 2007493, at *7. **While this Court is fully cognizant of the logistical and administrative challenges of managing a case with numerous putative defendants, a number of whom may seek to file papers *pro se*, severing the putative defendants is no solution to ease the administrative burden of the cases. The Court therefore declines to sever the putative defendants at this time.**"

Magistrate Judges of this District other than Magistrate Judge Grewal issued early discovery orders in cases similar to the instant case while noting the joinder issue. In the Order issued by Chief Magistrate Judge Maria-Elena James on April 18, 2011 in Case No. CV 10-05863 MEJ, Document # 8, and in the Order issued by Magistrate Judge Joseph C. Spero on May 9, 2011 in Case No. CV 10-05885 JCS, Document # 13, both specifically noted with respect to the joinder issue (emphasis added),

"joinder of all defendants at this stage of the litigation is proper. This decision is without prejudice to any motion for severance by a current Doe defendant who is later included in this action by his or her true name."

As noted above, Plaintiff contends that Magistrate Judge Grewal missed the point in the cases he relied upon (CV 10-05865 PSG, ECF #16, pp. 6-7 and fn. 16 and 18-22), namely that the plaintiffs in those failed to contend that the Doe defendants acted in concert with each other. In BMG Music v. Does, No. C 06-01579 [Document #14], 2006 U.S. Dist. LEXIS 53237 (N.D. Cal. Jul. 31, 2006), Judge Marilyn Hall Patel explained the basis of her ruling and the ruling in the Twentieth Century Fox case:

"The only connection between defendants noted by plaintiffs' papers is the fact that defendants allegedly used the same ISP, Covad Communications, to conduct the infringing acts. Mot. at 2. However, absent any allegation that these individuals acted in concert, there is no basis for joinder.

"Numerous federal courts have found that joinder is improper when there is no allegation that multiple defendants acted in concert. See Twentieth Century Fox Film Corp. v. Does 1-12, No. C 04-04862 WHA (N.D. Cal. Nov. 16, 2004) (Alsup, J.) (severing multiple Doe defendants in a copyright infringement case where although defendants used the same ISP to allegedly infringe motion picture recordings, there was no allegation that the individuals acted in concert)"

In the case decided by Magistrate Judge Grewal, and in the instant case, the following allegation is in paragraph 11 of each Complaint,

//

"Each Defendant has acted in cooperation with the other Defendants by agreeing to provide, and actually providing, on a P2P network an infringing reproduction of at least substantial portions of Plaintiff's copyrighted Motion Picture, in anticipation of the other Defendants doing likewise with respect to that work and/or other works."

In the instant case, as explained in the Nicolini Declaration, the accused Doe Defendants act, and must act, cooperatively to distribute unlawful copies of the copyrighted work.

While Plaintiff uses the phrase "in cooperation" as opposed to "in concert," those phrases are synonymous. See, <http://www.merriam-webster.com/dictionary/cooperate>.

In another "swarm" copyright infringement case decided by Judge Howell, namely Voltage Pictures, LLC v. Does 1-5000, D.D.C. Case No. CV 10-0873 BAH³, in Document #150, a copy of which is attached hereto as **Exhibit 9**, the court distinguishes the other cases cited by Magistrate Judge Grewal and others as well, and acknowledges that BitTorrent file sharing uses a "swarm" of infringers. In that case, the court denied motions to quash by several defendants. At pages 14-16 Judge Howell explained as follows:

"Some courts in other jurisdictions have granted motions by putative defendants for severance in analogous copyright infringement cases against unknown users of peer-to-peer file-sharing programs for failure to meet the 'same transaction or occurrence test' in Rule 20(a)(2). Those courts have been confronted with bare allegations that putative defendants used the same peer-to-peer network to infringe copyrighted works and found those allegations were insufficient for joinder. See, e.g., IO Grp., Inc. v. Does 1-19, No. 10-03851, 2010 WL 5071605, at *8-12 (N.D. Cal. Dec. 7, 2010); Arista Records, LLC v. Does 1-11, No. 07-cv-2828, 2008 WL 4823160, at *6 (N.D. Ohio Nov. 3, 2008) ('merely alleging that the Doe Defendants all used the same ISP and file-sharing network to conduct copyright infringement without asserting that they acted in concert was not enough to satisfy the same series of transactions requirement under the Federal Rules.');

LaFace Records, LLC v. Does 1-38, No. 5:07-cv-298, 2008 WL 544992, at *3 (E.D. N.C. Feb. 27, 2008) (severing putative defendants in file-sharing case not involving BitTorrent technology, noting that 'other courts have commonly held that where there is no assertion that multiple defendants have acted in concert, joinder is improper.');

Interscope Records v. Does 1-25, No. 6:04-cv-197, 2004 U.S. Dist. LEXIS 27782 (M.D. Fla. Apr. 1, 2004) (adopting Mag. J. Report and Recommendation at Interscope Records v. Does 1-25, No. 6:04-cv-197, 2004 U.S. Dist. LEXIS 27782 (M.D. Fla. Apr. 1, 2004)). That is not the case here.

"The plaintiff has provided detailed allegations about how the BitTorrent technology differs from other peer-to-peer file-sharing programs and necessarily engages many users simultaneously or sequentially to operate. See Columbia Pictures Indus. v. Fung, No. 06-5578, 2009 U.S. Dist. LEXIS 122661, at *7 (C.D.

³ This case, too, was cited with approval in MCGIP, LLC v. Does 1-18, Northern District of California Case No. CV 11-1495 EMC (N.D. Cal. June 2, 2011) (Doc. #14), by United States District Judge Edward M. Chen.

Cal. Dec. 21, 2009) (BitTorrent 'is unique from that of previous [P2P] systems such as Napster and Grokster. Rather than downloading a file from an individual user, [BitTorrent users download] from a number of host computers that possess the file simultaneously. . . . The BitTorrent client application simultaneously downloads the pieces of the content file from as many users as are available at the time of the request, and then reassembles the content file on the requesting computer when the download is complete. Once a user downloads a given content file, he also becomes a source for future requests and downloads.'). Specifically, BitTorrent creates a 'swarm' in which 'each additional user becomes a part of the network from where the file can be downloaded . . . [U]nlike a traditional peer-to-peer network, each new file downloader is receiving a different piece of the data from each user who has already downloaded the file that together comprises the whole.' Second Am. Compl., ¶ 3.

"At least one court has not been persuaded that allegations of copyright infringement by users of BitTorrent satisfy the requirement of Rule 20. See, e.g., Lightspeed v. Does 1-1000, No. 10-cv-5604, 2011 U.S. Dist. LEXIS 35392, at *4-7 (N.D. Ill. Mar. 31, 2011) (finding that Doe defendants using BitTorrent technology were misjoined on the basis that the putative defendants were not involved in the 'same transaction, occurrence, or series of transactions or occurrence' under FED. R. CIV. P. 20(a)(2)(A)); Millennium TGA Inc. v. Does 1-800, No. 10-cv-5603, 2011 U.S. Dist. LEXIS 35406, at *3-5 (N.D. Ill. Mar. 31, 2011) (same). In those cases, the court did not discuss the precise nature of the BitTorrent technology, which enables users to contribute to each other's infringing activity of the same work as part of a 'swarm.' In any event, by contrast to the instant claim of infringement of a single copyrighted work by the putative defendants, the plaintiffs in Lightspeed and Millennium TGA Inc. alleged infringement of multiple works, a factor that may undermine the requisite showing of concerted activity to support joinder.

Here, as in Voltage Pictures, Plaintiff alleges that the Doe defendants have acted in cooperation with each other (i.e., in concert), and Plaintiff's expert, Nicolini, explained (here par. 6 is repeated for convenience),

"P2P networks distribute infringing copies of motion pictures (and works in other forms such as music and books) with file sharing software such as BitTorrent as follows: The process begins with one user accessing the Internet through an Internet Service Provider ('ISP') and intentionally making a digital file of the work available on the Internet to the public from his or her computer. This first file is often referred to as the first 'seed.' I will refer to the person making this seed available as the 'original seeder.' Persons seeking to download such a work also access the Internet through an ISP (which may or may not be the same ISP as used by the original seeder) and seek out the work on a P2P network. With the availability of the seed, other users, who are referred to as 'peers,' access the Internet and request the file (by searching for its title or even searching for the torrent's 'hash' - described below) and engage the original seeder and/or each other in a group, sometimes referred to as a 'swarm,' and begin downloading the seed file. In turn, as each peer receives portions of the seed, most often that peer makes those portions available to other peers in the swarm. Therefore, each peer in the swarm is at least copying and is usually distributing, as a follow-on seeder, copyrighted material at the same time. Of the over 20,000 infringers tracked in connection with several cases currently pending, at least 95% of the Doe defendants were uploading (i.e., distributing) illegal copies of our clients' motion pictures at the moment indicated by the Timestamp in the respective Exhibit A

1 appended to each complaint. In P2P networks, the infringement may continue
 2 even after the original seeder has gone completely offline. Any BitTorrent client
 3 may be used to join a swarm. As more peers join a swarm at any one instant, they
 4 obtain the content at even greater speeds because of the increasing number of
 5 peers simultaneously offering the content as seeders themselves for unlawful
 6 distribution. As time goes on, the size of the swarm varies, yet it may endure for
 7 a long period. As a result, the original seed file becomes unlawfully duplicated
 8 multiple times by multiple parties, with a potentially exponential increase in the
 9 number of illegal copies of any copyrighted work. With respect to any particular
 10 swarm, the hash (an alphanumeric representation of a digital file) associated with
 11 the copied file's torrent file remains the same."

12 In MCGIP, LLC v. Does 1–18, Northern District of California Case No. CV 11-1495
 13 EMC (N.D. Cal. June 2, 2011) (Doc. #14), United States District Judge Edward M. Chen held:

14 Fourth, Doe's assertion of improper joinder may be meritorious but, '[a]t this
 15 stage in the litigation, . . . when discovery is underway [only] to learn identifying
 16 facts necessary to permit service on Doe defendants, joinder . . . of unknown
 17 parties identified only by IP addresses is proper,' particularly where, are here, the
 18 complaint contains allegations that the Doe Defendants have infringed Plaintiff's
 19 copyright through 'the same file-sharing software program [i.e., BitTorrent] that
 20 operates through simultaneous and sequential computer connections and data
 21 transfers among the users.' *Voltage*, 2011 U.S. Dist. LEXIS 50787, at *29. Doe
 22 may, at a later point in this litigation, raise the joinder issue if Plaintiff maintains
 23 this action against him or her.

24 Plaintiff submits that, in view of the foregoing, Magistrate Judge Grewal's dismissal for
 25 improper joinder recommendation in Diabolic Video Productions, Inc. v. Does 1-2099, 10-CV-
 26 05865-PSG, Docket No. 16 (N.D. Cal. 2011) is without merit, particularly at this stage of the
 27 litigation.

28 IV. EVEN IF, FOR THE SAKE OF ARGUMENT, THE RULING IN *LIGHTSPEED*
V. DOES 1-1000, 2011 U.S. Dist. LEXIS 35392 24 (N.D. Ill. 2011) WERE
 CORRECT, IT DOES NOT RELATE TO THE INSTANT CASE

Lightspeed v. Does 1-1000, 2011 U.S. Dist. LEXIS 35392 24 (N.D. Ill. 2011) is not
 analogous to the instant case. In Lightspeed the plaintiff sued Doe defendants for infringement
 of multiple works (see the cited opinion's reference to "creative works" and the first amended
 complaint in that action (Doc.#21 in Northern District of Illinois Case No. 10-cv-05604), and
 plaintiff gave no good faith basis for its allegation that it believed any of the defendants were
 located in Illinois.

In the instant case, only one work is involved, and only a single "swarm" is involved.
 Further, Plaintiff's expert testified,

"[W]e could determine that of the 5011 Doe Defendants in this case, at least 1 out of every 7 of the IP addresses is likely associated with physical address in California, and of those more than 1 out of every 5 is likely in one of the counties within the Northern District of California (i.e., Alameda, Contra Costa, Del Norte, Humboldt, Lake, Marin, Mendocino, Monterey, Napa, San Benito, San Francisco, San Mateo, Santa Clara, Santa Cruz, or Sonoma county). However, without information held by the ISPs, we cannot obtain further information needed to identify the Defendants, including their names, and their actual addresses, telephone numbers and email addresses."

Nicolini Decl., par. 23.

Lightspeed was distinguished in Maverick Entertainment Group, Inc. v. Does 1-2,115, D.D.C. Case No. CV 10-0569 BAH (N.D. Ill. May 12, 2011) (Doc.#133), a copy of which is attached hereto as Exhibit 14:

"At least one court has not been persuaded that allegations of copyright infringement by users of BitTorrent satisfy the requirement of Rule 20. *See, e.g., Lightspeed v. Does 1-1000*, No. 10-cv-5604, 2011 U.S. Dist. LEXIS 35392, at *4-7 (N.D. Ill. Mar. 31, 2011) (finding that Doe defendants using BitTorrent technology were misjoined on the basis that the putative defendants were not involved in the 'same transaction, occurrence, or series of transactions or occurrence' under FED. R. CIV. P. 20(a)(2)(A)); *Millennium TGA Inc. v. Does 1-800*, No. 10-cv-5603, 2011 U.S. Dist. LEXIS 35406, at *3-5 (N.D. Ill. Mar. 31, 2011) (same). In those cases, the court did not discuss the precise nature of the BitTorrent technology, which enables users to contribute to each other's infringing activity of the same work as part of a 'swarm.' Similarly to the instant claims of infringement of thirteen copyrighted works by the putative defendants, the plaintiffs in *Lightspeed* and *Millennium TGA Inc.* alleged infringement of multiple works. Indeed, concluding that the allegations against the putative defendants in this case stem from the same transaction, or series of transactions is made more complicated by the fact that the plaintiff claims infringement of thirteen separate movies. This is a factor that may undermine the requisite showing of concerted activity to support joinder when the plaintiff identifies and names defendants to this action. *See Fonovisa, Inc. v. Does 1-9*, 2008 WL 919701, at *6 (W. D. Pa. April 3, 2008) (Misjoinder found in copyright infringement case where '[n]one of the Defendants downloaded and/or distributed the same copyrighted recordings belonging to the same set of Plaintiffs, and each of the Defendants accessed a different number of audio files on different dates); *See Bridgeport Music, Inc. v. IIC Music*, 202 F.R.D. 229, 232 (M.D. Tenn. 2001) (severing defendants accused of sampling different songs and stating that sampling of each song represented a 'discrete occurrence' and that 'the Court is not persuaded by Plaintiffs' argument that its infringement counts are properly joined because Plaintiffs suffered the same harm in each instance. According to this logic, a copyright plaintiff could join as defendants any otherwise unrelated parties who independently copy material owned by the plaintiff.'). The Court is guided, however, by the principle that permissive joinder seeks the 'broadest possible scope of action,' *Gibbs*, 383 U.S. at 724, particularly when there are no named defendants and the putative defendants are not harmed by joinder at this stage. Should the defendants be named and make motions for severance, the plaintiff will be required to

demonstrate with greater specificity the relatedness of the named defendants' alleged conduct and the factual basis for joinder under Rule 20(a)(2)(A)."

Lightspeed was also distinguished in by a sister court in the Northern District of Illinois in MGCIP [sic] v. Does 1 - 316, Northern District of Illinois Case No. CV 10-06677 (N.D. Ill. June 9, 2011) (Doc. #133), a copy of which is attached hereto as Exhibit 15:

"Plaintiff MCGIP, LLC ("MCGIP") filed suit against putative defendants John Does 1-316 alleging copyright infringement through the use of the BitTorrent protocol.

* * *

"The Court also finds that the putative defendants' arguments that they were improperly joined are premature. See *Donkeyball*, --- F.Supp.2d ----, 2011 WL 1807452 at *4 ('At this stage in the litigation . . . when discovery is underway to learn identifying facts necessary to permit service on Doe defendants, joinder, under Federal Rule of Civil Procedure 20(a)(2), of unknown parties identified only by IP addresses is proper.'). The putative defendants may re-raise the issue of improper joinder should they become named defendants in this case. See *MCGIP*, 2011 WL 2181620 at *1 ('Doe's assertion of improper joinder may be meritorious but, at this stage in the litigation, when discovery is underway only to learn identifying facts necessary to permit service on Doe defendants, joinder of unknown parties identified by IP addresses is proper.') (quotations and citation omitted).¹¹ While a court in this district has granted a motion to sever regarding a copyright infringement case alleging the use of a BitTorrent protocol, it did so after finding that the claims against the putative defendants did not arise out of the same transaction or occurrence. See, e.g., *Lightspeed v. Does 1-1000*, 2011 LEXIS 35392 at *4 (N.D. Ill. Mar. 31, 2011) (Manning, J.) (sua sponte concluding that the putative defendants were improperly joined). Here, however, given the decentralized nature of BitTorrent's file-sharing protocol—where individual users distribute the same work's data directly to one another without going through a central server—the Court finds that sufficient facts have been plead to support the joinder of the putative defendants at this time. See, e.g., *Donkeyball*, --- F.Supp.2d ----, 2011 WL 1807452 at *8 (finding joinder proper and collecting cases holding that severance prior to the naming of the actual defendants was premature)."

So, in the instant case, in which a single work has been infringed by Doe defendants cooperating together on a BitTorrent network in a single swarm, Lightspeed provides no basis for severance of any defendant at this stage of the litigation.

//

//

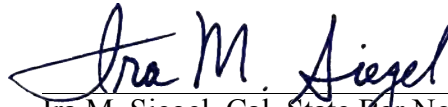
//

V. CONCLUSION

In view of the foregoing, Plaintiff submits that the Court should vacate its Order to Show Cause.

Respectfully submitted,

Date: July 13, 2011



Ira M. Siegel, Cal. State Bar No. 78142
email address: irasiegel@earthlink.net
LAW OFFICES OF IRA M. SIEGEL
433 N. Camden Drive, Suite 970
Beverly Hills, California 90210-4426
Tel: 310-435-7656
Fax: 310-657-2187

Attorney for Plaintiff On The Cheap, LLC DBA Tru Filth,
LLC

Exhibit 2

to

Plaintiff's Response to Order to Show Cause - CV 10-04472 BZ

On The Cheap, LLC DBA Tru Filth, LLC v. Does 1-5011, Case No. CV 10-04472 BZ

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

<div>CALL OF THE WILD MOVIE, LLC,</div> <div>Plaintiff,</div> <div>v.</div> <div>DOES 1-1,062,</div> <div>Defendants.</div>	<div>Civil Action No. 10-455 (BAH)</div> <div>Judge Beryl A. Howell</div>
<div>MAVERICK ENTERTAINMENT GROUP, INC.,</div> <div>Plaintiff,</div> <div>v.</div> <div>DOES 1-4,350,</div> <div>Defendants.</div>	<div>Civil Action No. 10-569 (BAH)</div> <div>Judge Beryl A. Howell</div>
<div>DONKEYBALL MOVIE, LLC,</div> <div>Plaintiff,</div> <div>v.</div> <div>DOES 1-171,</div> <div>Defendants.</div>	<div>Civil Action No. 10-1520 (BAH)</div> <div>Judge Beryl A. Howell</div>

MEMORANDUM OPINION

Currently before the Court are Time Warner Cable’s (hereinafter “Time Warner”) Motions to Quash or Modify subpoenas that were issued in three pending copyright infringement cases: *Call of the Wild Movie, LLC v. Does 1-1,062*, No. 10-cv-455 (hereinafter “*Wild*”); *Maverick Entertainment Group, Inc. v. Does 1-4,350*, No. 10-cv-569 (hereinafter “*Maverick*”); and *Donkeyball Movie, LLC v. Does 1-117*, No. 10-cv-1520 (hereinafter “*Donkeyball*”). In the interest of judicial economy, this Memorandum Opinion will address and resolve the issues

related to Time Warner's motions to quash pending before the Court in all three of the captioned actions. In so doing, however, the Court emphasizes that these cases have not been consolidated for any purpose. This Memorandum Opinion, moreover, should in no way leave the parties with the impression that the Court views these cases as inextricably related; rather, with respect to Time Warner's pending motions to quash, the relevant factual allegations, legal theories and asserted burdens are the same and may be addressed in a unitary opinion.

Time Warner claims that the subpoenas issued to it in each of the three cases should be quashed due to the undue burden that Time Warner faces with compliance. *Wild*, ECF No. 7, May 13, 2010; *Maverick*, ECF No. 18, Nov. 22, 2010; *Donkeyball*, ECF No. 7, Dec. 13, 2010. Alternatively, Time Warner argues that the subpoenas should be substantially modified to require production of the requested information on a schedule that would likely take about three years. *See* Time Warner Mem. Supp. Mot. Quash, *Wild*, at 11, ECF No. 7 (requesting the Court to modify subpoena to limit Time Warner's production responsibilities to 28 IP addresses a month); *see generally* Time Warner Mem. Supp. Mot. Quash, *Maverick*, ECF No. 18, at 4-5; Time Warner Mem. Supp. Mot. Quash, *Donkeyball*, ECF No. 7, at 4-5. After reviewing Time Warner's Motions, the plaintiffs' opposition papers, the amicus briefs, supplemental filings, as well as the accompanying declarations and applicable law, the Court denies Time Warner's motions to quash in *Wild* and *Donkeyball* and grants Time Warner's Motion to Quash in *Maverick* because the plaintiff failed to serve Time Warner with its subpoena in accordance with Federal Rule of Civil Procedure 45(b).

I. FACTUAL AND PROCEDURAL BACKGROUND

Wild, *Maverick*, and *Donkeyball* are cases in which copyright owners of separate movies allege that their copyrights are being infringed in the same manner. Specifically, the plaintiffs

allege that varying numbers of defendants, who are currently unnamed, are illegally downloading and distributing copyrighted works using a file-sharing protocol called BitTorrent. In *Wild*, the Amended Complaint, filed on May 12, 2010, accuses 1,062 unnamed Doe defendants of infringing the copyright of the motion picture *Call of the Wild*. *Wild*, ECF No. 6. In *Maverick*, the Amended Complaint, filed on August 10, 2010, accuses 4,350 unnamed Doe defendants of infringing the copyrights of the motion pictures *13 Hours in a Warehouse*, *A Numbers Game*, *Border Town*, *Deceitful Storm*, *Fast Track No Limits*, *He Who Finds a Wife*, *Hellbinders*, *Locator 2*, *Smile Pretty (aka Nasty)*, *Stripper Academy*, *The Casino Job*, *The Clique (aka Death Clique)*, and *Trunk*. *Maverick*, ECF No. 9. In *Donkeyball*, the Complaint, filed on September 8, 2010, accuses 171 unnamed Doe defendants of infringing the copyrights of the motion picture *Familiar Strangers*. *Donkeyball*, ECF No. 1.

The putative defendants in each case are alleged to have used a file sharing protocol called BitTorrent, which allows users to share files anonymously with other users. When a user downloads a specific file through BitTorrent -- in this case, plaintiffs' copyrighted motion pictures -- data is transferred in a "piecemeal" fashion whereby "a different piece of the data [is received] from each user who has already downloaded the file" Amended Compl., *Wild*, ¶ 3, ECF No. 6; Amended Compl., *Maverick*, ¶ 3, ECF No. 9; Compl., *Donkeyball*, ¶ 3, ECF No. 1; *see also* Pl.'s Mot. Leave to Take Disc. Prior to Rule 26(f) Conference, *Wild*, ECF No. 2, Benjamin Perino Decl., ¶¶ 7-8; Pl.'s Mot. Leave to Take Disc. Prior to Rule 26(f) Conference, *Maverick*, ECF No. 4, Benjamin Perino Decl., ¶¶ 7-8; Pl.'s Mot. Leave to Take Disc. Prior to Rule 26(f) Conference, *Donkeyball*, ECF No. 4, Benjamin Perino Decl., ¶¶ 7-8. The nature of the BitTorrent file-sharing technology "makes every downloader also an uploader of the illegally transferred file(s)." Amended Compl., *Wild*, ¶ 3, ECF No. 6; Amended Compl., *Maverick*, ¶ 4,

ECF No. 9; Compl., *Donkeyball*, ¶ 4, ECF No. 1. Since users download material from a number of other individuals, “every infringer is simultaneously stealing copyrighted material from many ISPs in numerous jurisdictions around the country.” Amended Compl., *Wild*, ¶ 4, ECF No. 6; Amended Compl., *Maverick*, ¶ 4, ECF No. 9; Compl., *Donkeyball*, ¶ 4, ECF No. 1.

In an effort to combat illegal transfer of their copyrighted movies, the plaintiffs in *Wild*, *Maverick*, and *Donkeyball* contracted with Guardaley Limited, an anti-piracy firm that uses proprietary technology to identify BitTorrent users sharing the plaintiffs’ copyrighted works. See Pl.’s Mot. Leave to Take Disc. Prior to Rule 26(f) Conference, *Wild*, ECF No. 2, Benjamin Perino Decl., ¶ 10.¹ The plaintiffs assert that Guardaley was able to identify the users that were illegally sharing the plaintiffs’ motion pictures, and then provided the plaintiffs with the alleged infringers’ Internet Protocol (IP) addresses, as well as the date and time the alleged infringement activity occurred. *Id.*; see also Pl.’s Mot. Leave to Take Disc. Prior to Rule 26(f) Conference, *Wild*, ECF No. 2, Patrick Achache Decl., at ¶¶ 13-14. The difficulty for the plaintiffs, however, is that they have no identifying information for these alleged infringers aside from the IP addresses that Guardaley supplied.

To obtain certain identifying information for the putative defendants, plaintiffs moved for expedited discovery. Pl.’s Mot. Leave to Take Disc. Prior to Rule 26(f) Conference, *Wild*, ECF No. 2; Pl.’s Mot. Leave to Take Disc. Prior to Rule 26(f) Conference, *Maverick*, ECF No. 4; Pl.’s Mot. Leave to Take Disc. Prior to Rule 26(f) Conference, *Donkeyball*, ECF No. 4. The Court in each case granted plaintiffs leave to subpoena Internet Service Providers (ISPs) to compel production of the names, addresses, emails, phone numbers, and Media Access Control numbers

¹ For clarity, this opinion will cite primarily to material docketed in *Wild*, No. 10-cv-455. Plaintiffs are represented by the same counsel, and the plaintiffs and Time Warner’s briefs and filings in *Wild*, *Maverick*, and *Donkeyball* generally assert the same claims and factual matters, differing only in the copyrighted material at issue, the putative defendants and, in *Maverick*, assertion of a jurisdictional basis for quashing the subpoena. Any other differences will be noted in the opinion.

associated with the alleged infringing IP addresses that the plaintiffs identified as engaging in infringing distribution of their respective movies. Order Granting Pl.'s Mot. for Leave to Take Disc. Prior to Rule 26(f) Conference, *Wild*, Apr. 15, 2010, ECF No. 4 (Urbina, J.); Order Granting Pl.'s Mot. for Leave to Take Disc. Prior to Rule 26(f) Conference, *Maverick*, No. 10-569, May, 24 2010, ECF No. 7 (Leon, J.); Order Granting Pl.'s Mot. for Leave to Take Disc. Prior to Rule 26(f) Conference, *Donkeyball*, Oct. 19, 2010, ECF No. 6 (Sullivan, J.). Time Warner received subpoenas for information relating to 224 Time Warner subscribers in *Wild*, 783 subscribers in *Maverick*, and 21 subscribers in *Donkeyball*. Time Warner Mot. Quash, *Wild*, ECF No. 7, Ex. 1; Time Warner Mot. Quash, *Maverick*, ECF No. 18, Ex. 1; Time Warner Mot. Quash, *Donkeyball*, ECF No. 7, Ex. 1. Time Warner responded by moving to quash the subpoenas on grounds that producing the requested information would impose an undue burden and expense. *Wild*, May 13, 2010, ECF No. 7; *Maverick*, Nov. 22, 2010, ECF No. 18; *Donkeyball*, Dec. 13, 2010, ECF No. 7. In support of Time Warner's motion to quash in *Wild*, amicus briefs were submitted collectively by Electronic Frontier Foundation, Public Citizen, American Civil Liberties Union Foundation, and American Civil Liberties Union of the Nation's Capital. Minute Order, *Wild*, dated Jan. 3, 2011 (granting Amici leave to file amicus brief) (Urbina, J.). Amici urge the Court to quash the subpoena issued to Time Warner based upon improper joinder, lack of personal jurisdiction over the putative defendants, and the putative defendants' First Amendment right to anonymity.

Following re-assignment to this Court, on March 1, 2011, the Court held a joint conference in these cases to hear oral argument on Time Warner's motions. Time Warner,

Amici, the plaintiffs, and an attorney representing three putative defendants participated.² At the conference, the Court stated that it would accept supplemental filings in the case in order to more fully develop the record on the burdens faced by Time Warner.³ See Minute Order, *Wild*, March 9, 2011. Amici, plaintiffs, and Time Warner each filed supplemental material.

If the Court were to accept the Amici's arguments, not only would the Court quash the subpoenas directed toward Time Warner, but plaintiffs' cases would face significant obstacles.⁴ For this reason, the Court addresses Amici's contentions before turning to Time Warner's arguments in support of quashing or modifying the plaintiffs' subpoenas.

II. AMICI'S CONTENTION THAT THE PUTATIVE DEFENDANTS ARE IMPROPERLY JOINED

Amici argue that the Court should quash the subpoenas directed to Time Warner because the plaintiffs have improperly joined the putative defendants. See FED. R. CIV. P. 20(a)(2). For the reasons stated below, the Court finds that the plaintiffs' allegations against the putative defendants in each case meet the requirements for permissive joinder. After the putative

² Counsel identified his clients in *Maverick* as Lori Pearlman, Calvin Johnson, and Xu Xiangping. Transcript of Mot. Hearing, at 52-53, *Call of the Wild Movie LLC v. Does 1-1,063*, No. 10-cv-455 (Mar. 1, 2011)

³ Counsel for Time Warner was unable to address certain questions posed by the Court during oral argument on Time Warner's Motions to Quash:
 "MR. MALTAS: Well, as to the specifics of what's done in each location, I grant I'm not sure I can answer the question of what is done specifically at the central office and what is done specifically at regional offices. I do know that it requires work at both, and it requires --...-- people at both.
 THE COURT: One of the declarations said that at the regional office, it takes about 20 minutes per IP look-up to do something, but it doesn't exactly explain ... what takes 20 minutes per IP look-up? What are they doing that takes 20 minutes?
 MR. MALTAS: I don't want to give an answer that is not technically correct, and I don't know the answer to that, so I can go back and we can file a supplemental affidavit, if that would help the Court."
 Transcript of Mot. Hearing, at 27-28, *Call of the Wild Movie LLC v. Does 1-1,063*, No. 10-cv-455 (Mar. 1, 2011).

⁴ Time Warner also raises the argument that its burdens are caused by the plaintiffs' "failure to observe jurisdictional limitations and improper joinder." Time Warner Mem. Supp. Mot. Quash, *Maverick*, at 13-15 (addressing joinder and personal jurisdiction issues); Time Warner Mem. Supp. Mot. Quash, *Donkeyball*, at 13-15 (addressing joinder and personal jurisdiction issues); see also Time Warner Mem. Supp. Mot. Quash, *Wild*, at 10 (addressing joinder). Time Warner does not argue, however, that it is precluded from producing its subscribers' identifying information due to the putative defendants' First Amendment right to anonymity. The Court addresses these issues *sua sponte* under its duty to supervise discovery in these cases. See FED. R. CIV. P. 26(b)(2)(C) ("On motion or *on its own*, the court must limit the frequency or extent of discovery otherwise allowed by these rules...")(emphasis added).

defendants have been identified and named in the Complaints, the defendants may raise the argument that they are improperly joined under Federal Rule of Civil Procedure 20 and move to sever the joined defendants under Federal Rule of Civil Procedure 21. Severance at this stage, however, as numerous other courts both in and outside this District have held, is premature. *See, e.g., Achte/Neunte Boll Kino Beteiligungs GMBH & Co, KG v. Does 1 - 4*, 577, No. 10-cv-00453, ECF No. 34 (D.D.C. July 2, 2010) (Collyer, J.); *West Bay One, Inc. v. Does 1-1653*, No. 10-cv-00481, ECF No. 25 (D.D.C. July 2, 2010) (Collyer, J.); *Arista Records LLC v. Does 1-19*, 551 F. Supp. 2d 1, 11 (D.D.C. 2008) (Kollar-Kotelly, J.); *London-Sire Records, Inc. v. Doe 1*, 542 F. Supp. 2d 153, 161 n.7 (D. Mass. 2008); *Sony Music Entm't, Inc. v. Does 1-40*, 326 F. Supp. 2d 556, 568 (S.D.N.Y. 2004).

A. LEGAL STANDARD

Under the Federal Rules of Civil Procedure, defendants may be joined in one action when claims arise from the same transaction or occurrence or series of transactions or occurrences; and any question of law or fact in the action is common to all defendants. FED. R. CIV. P. 20(a)(2); *see also Montgomery v. STG Int'l, Inc.*, 532 F. Supp. 2d 29, 35 (D.D.C. Jan. 30, 2008) (interpreting Rule 20(a)(1), which has the same requirements as Rule 20(a)(2)).

Permissive joinder is appropriate “to promote trial convenience and expedite the final resolution of disputes, thereby preventing multiple lawsuits, extra expense to the parties, and loss of time to the court as well as the litigants appearing before it.” *M.K. v. Tenet*, 216 F.R.D. 133, 137 (D.D.C. 2002). The requirements for permissive joinder are “liberally construed in the interest of convenience and judicial economy in a manner that will secure the just, speedy, and inexpensive determination of the action.” *Lane v. Tschetter*, No. 05-1414, 2007 WL 2007493, at *7 (D.D.C. July 10, 2007) (quoting *Jonas v. Conrath*, 149 F.R.D. 520, 523 (S.D. W.Va. 1993));

see also Davidson v. District of Columbia, 736 F. Supp. 2d 115, 119 (D.D.C. 2010). Thus, “the impulse is toward entertaining the broadest possible scope of action consistent with fairness to the parties; [and] joinder of claims, parties, and remedies is strongly encouraged.” *United Mine Workers of Am. v. Gibbs*, 383 U.S. 715, 724 (1966).

The remedy for improper joinder is severance under Federal Rule of Civil Procedure 21. This rule does not set forth what constitutes misjoinder, but “it is well-settled that parties are misjoined when the preconditions of permissive joinder set forth in Rule 20(a) have not been satisfied.” *Disparte v. Corporate Exec. Bd.*, 223 F.R.D. 7, 12 (D.D.C. 2004) (quoting *Puricelli v. CNA Ins. Co.*, 185 F.R.D. 139, 142 (N.D.N.Y. 1999)). Courts have also read Rule 21 in conjunction with Rule 42(b), which allows the court to sever claims in order to avoid prejudice to any party. *Tenet*, 216 F.R.D. at 138 (citing *Brereton v. Commc'ns Satellite Corp.*, 116 F.R.D. 162, 163 (D.D.C.1987)); *see also* FED. R. CIV. P. 42(b) (“For convenience, to avoid prejudice, or to expedite and economize, the court may order a separate trial of one or more separate issues, claims, crossclaims, counterclaims, or third-party claims.”). In addition to the two requirements of Rule 20(a)(2), the Court therefore also considers whether joinder would prejudice any party or result in needless delay. *See Lane*, 2007 WL 2007493, at *7; *Tenet*, 216 F.R.D. at 138.

B. DISCUSSION

Consideration of the two requirements for permissive joinder under Rule 20(a)(2) and their application to the allegations in the Complaints in *Wild*, *Maverick*, and *Donkeyball* make clear that, at this procedural juncture, joinder of the putative defendants is proper. Joinder will avoid prejudice and needless delay for the only party currently in the case, namely the plaintiff, and promote judicial economy.

1. Same Transaction, Occurrence, or Series of Transactions or Occurrences

Rule 20(a)(2)(A) states that joinder is proper if “any right to relief is asserted against [the joined defendants] jointly, severally, or in the alternative with respect to or arising out of the same transaction, occurrence, or series of transactions or occurrences.” This essentially requires claims asserted against joined parties to be “logically related.” *Disparte*, 223 F.R.D. at 10. This is a flexible test and courts seek the “broadest possible scope of action.” *Lane*, 2007 WL 2007493, at *7 (quoting *Gibbs*, 383 U.S. at 724). In the present case, the plaintiffs allege that the putative defendants in each case used the BitTorrent file-sharing protocol to illegally distribute the plaintiffs’ motion pictures. Amended Compl., *Wild*, ECF No. 6, ¶12. Amici counter, however, that engaging in “separate but similar behavior by individuals allegedly using the Internet to commit copyright infringement” does not satisfy Rule 20(a)(2)(A)’s requirement that the claim asserted against the joined defendants arise out of the same transaction, occurrence, or series of transactions or occurrences. Mem. of Amici Curiae Electronic Frontier Foundation, Public Citizen, American Civil Liberties Union Foundation and American Civil Liberties Union of the Nation’s Capital in Supp. Time Warner’s Mot. Quash, *Wild* (hereinafter “Amici Mem.”), at 11-12, ECF No. 18. Despite Amici’s arguments, at this nascent stage of the case, the plaintiffs have sufficiently alleged that the infringing activity at issue in each of the cases may involve multiple computers, based in various jurisdictions, which are using the BitTorrent protocol to make available for sharing the same copyrighted content.

Specifically, the plaintiffs allege that the BitTorrent file-sharing protocol “makes every downloader also an uploader of the illegally transferred file(s). This means that every “node” or peer user who has a copy of the infringing copyrighted material on a torrent network must necessarily also be a source of download for that infringing file.” Amended Compl., *Wild*, ¶3, ECF No. 6. The plaintiffs further assert that the “nature of a BitTorrent protocol [is that] any

seed peer that has downloaded a file prior to the time a subsequent peer downloads the same file is automatically a source for the subsequent peer so long as that first seed peer is online at the time the subsequent peer downloads a file.” *Id.* at ¶ 4.

Based on these allegations, the plaintiffs’ claims against the defendants are logically related. Each putative defendant is a possible source for the plaintiffs’ motion pictures, and may be responsible for distributing the motion pictures to the other putative defendants, who are also using the same file-sharing protocol to copy the identical copyrighted material. *See Disparte*, 223 F.R.D. at 10 (to satisfy Rule 20(a)(2)(A) claims must be “logically related” and this test is “flexible.”). While the defendants may be able to rebut these allegations later, the plaintiffs have sufficiently alleged that their claims against the defendants potentially stem from the same transaction or occurrence, and are logically related. *See Arista Records LLC v. Does 1-19*, 551 F. Supp. 2d 1, 11 (D.D.C.) (“While the Courts notes that the remedy for improper joinder is severance and not dismissal, . . . the Court also finds that this inquiry is premature without first knowing Defendants’ identities and the actual facts and circumstances associated with Defendants’ conduct.”).

2. *Question of Law or Fact Common to All Defendants*

Rule 20(a)(2)(B) requires the plaintiffs’ claims against the putative defendants to contain a common question of law or fact. *See Disparte*, 223 F.R.D. at 11. The plaintiffs meet this requirement. In each case, the plaintiff will have to establish against each putative defendant the same legal claims concerning the validity of the copyrights in the movies at issue and the infringement of the exclusive rights reserved to the plaintiffs as copyright holders.

Furthermore, the plaintiffs allege that the putative defendants utilized the same BitTorrent file-sharing protocol to illegally distribute and download the plaintiffs’ motion pictures and,

consequently, factual issues related to how BitTorrent works and the methods used by plaintiffs to investigate, uncover and collect evidence about the infringing activity will be essentially identical for each putative defendant. Amended Compl., *Wild*, ¶ 3; Amended Compl., *Maverick*, ¶ 3; Compl., *Donkeyball*, ¶ 3.

The Court recognizes that each putative defendant may later present different factual and substantive legal defenses but that does not defeat, at this stage of the proceedings, the commonality in facts and legal claims that support joinder under Rule 20(a)(2)(B).

3. *Prejudice to Any Party or Needless Delay*

Finally, the Court must assess whether joinder would prejudice the parties or result in needless delay. At this stage in the litigation, the Court believes it will not. To the contrary, joinder in a single case of the putative defendants who allegedly infringed the same copyrighted material promotes judicial efficiency and, in fact, is beneficial to the putative defendants. *See London-Sire Records, Inc. v. Doe I*, 542 F. Supp. 2d 153, 161 (D. Mass. 2008) (court consolidated separate Doe lawsuits for copyright infringement since the “cases involve similar, even virtually identical, issues of law and fact: the alleged use of peer-to-peer software to share copyrighted sound recordings and the discovery of defendants' identities through the use of a Rule 45 subpoena to their internet service provider. Consolidating the cases ensures administrative efficiency for the Court, the plaintiffs, and the ISP, and allows the defendants to see the defenses, if any, that other John Does have raised.”).

Notably, as part of the motion to modify the subpoena, Time Warner asks the Court to intervene in a cost dispute with plaintiffs' counsel and require payment for each IP address for which the subpoena requires identifying information rather than payment per customer. Time Warner Mem. Supp. Mot. Quash, *Wild*, at 12, ECF No. 7. The import of this request is that

some IP addresses may relate to the same person, who is engaged in the allegedly infringing activities claimed by plaintiffs. Severance of the putative defendants associated with different IP addresses may subject the same Time Warner customer to multiple suits for different instances of allegedly infringing activity and, thus, would not be in the interests of the putative defendants.

Moreover, the putative defendants are currently identified only by their IP addresses and are not named parties. Consequently, they are not required to respond to the plaintiffs' allegations or assert a defense. The defendants may be able to demonstrate prejudice once the plaintiffs proceed with their cases against them, but they cannot demonstrate any harm that is occurring to them before that time.

The plaintiffs, by contrast, are currently obtaining identifying information from ISPs so that they can properly name and serve the defendants. If the Court were to consider severance at this juncture, plaintiffs would face significant obstacles in their efforts to protect their copyrights from illegal file-sharers and this would only needlessly delay their cases. The plaintiffs would be forced to file 5,583 separate lawsuits, in which they would then move to issue separate subpoenas to ISPs for each defendant's identifying information. Plaintiffs would additionally be forced to pay the Court separate filing fees in each of these cases, which would further limit their ability to protect their legal rights. This would certainly not be in the "interests of convenience and judicial economy," or "secure a just, speedy, and inexpensive determination of the action." *Lane*, 2007 WL 2007493, at *7 (declining to sever defendants where "parties joined for the time being promotes more efficient case management and discovery" and no party prejudiced by joinder).

Given the administrative burden of simply obtaining sufficient identifying information to properly name and serve alleged infringers, it is highly unlikely that the plaintiffs could protect

their copyrights in a cost-effective manner. Indeed, Time Warner urges the Court to sever the defendants for this very reason. Time Warner asserts that, if joinder were disallowed, its burden of complying with subpoenas would be diminished because the plaintiffs would not be able to proceed against all of the putative defendants individually. *See* Transcript of Mot. Hearing, 14-16, *Call of the Wild Movie LLC v. Does 1-1,063*, No. 10-cv-455 (Mar. 1, 2011).

At this procedural juncture, the plaintiffs have met the requirements of permissive joinder under Rule 20(a)(2). The putative defendants are not prejudiced but likely benefited by joinder, and severance would debilitate the plaintiffs' efforts to protect their copyrighted materials and seek redress from the putative defendants who have allegedly engaged in infringing activity. Courts are instructed to "entertain[] the broadest possible scope of action consistent with fairness to the parties." *Lane*, 2007 WL 2007493, at *7. While this Court is fully cognizant of the logistical and administrative challenges of managing a case with numerous putative defendants, a number of whom may seek to file papers *pro se*, severing the putative defendants is no solution to ease the administrative burden of the cases. The Court therefore declines to sever the putative defendants at this time.

III. AMICI'S CONTENTION THAT THE COURT DOES NOT HAVE PERSONAL JURISDICTION OVER THE PUTATIVE DEFENDANTS

Amici further argue that the Court should quash the subpoenas issued to Time Warner because the plaintiffs have failed to properly establish personal jurisdiction over each putative defendant. Amici contend that the plaintiffs "failed to allege specific facts" to support jurisdiction and that the likelihood of the defendants uploading or downloading the plaintiffs' copyrighted movies in the District of Columbia is "exceedingly small." Amici Reply Brief, at 5-6, ECF No. 22. Given that the defendants have yet to be identified, the Court believes that evaluating the defendants' jurisdictional defenses at this procedural juncture is premature.

A. LEGAL STANDARD

To establish personal jurisdiction, the Court must examine whether jurisdiction is applicable under the District of Columbia's long-arm statute, D.C. CODE § 13-423, and must also determine whether jurisdiction satisfies the requirements of due process. *See GTE New Media Services Inc. v. BellSouth Corp.*, 199 F.3d 1343, 1347 (D.C. Cir. 2000). Due Process requires the plaintiff to show that the defendant has "minimum contacts" with the forum, thereby ensuring that "the defendant's conduct and connection with the forum State are such that he should reasonably anticipate being haled into court there." *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286, 297 (1980); *see also GTE New Media Servs.*, 199 F.3d at 1347.

In cases where a party's contacts with the jurisdiction are unclear and the record before the court is "plainly inadequate," courts have allowed for a discovery period within which to gather evidence to support jurisdiction. *See GTE New Media Servs.*, 199 F.3d at 1351-52 (reversing lower court's finding of personal jurisdiction, but stating that "[t]his court has previously held that if a party demonstrates that it can supplement its jurisdictional allegations through discovery, then jurisdictional discovery is justified."). "This Circuit's standard for permitting jurisdictional discovery is quite liberal," *Diamond Chem. Co. v. Atofina Chems., Inc.*, 268 F. Supp. 2d 1, 15 (D.D.C. 2003), and jurisdictional discovery is available when a party has "at least a good faith belief" that it has personal jurisdiction. *Caribbean Broad. Sys., Ltd. v. Cable & Wireless PLC*, 148 F.3d 1080, 1090 (D.C. Cir. 1998). Courts have permitted discovery even when a party has failed to establish a prima facie case of personal jurisdiction. *See GTE New Media Servs.*, 199 F.3d at 1351-52 ("... as the record now stands, there is absolutely no merit to [plaintiff]'s bold claim that the parent companies and subsidiaries involved in this lawsuit should be treated identically. Jurisdictional discovery will help to sort out these

matters.”); *see also In re Vitamins Antitrust Litigation*, 94 F. Supp. 2d 26, 35 (D.D.C. 2000) (discussing *GTE New Media Servs.* and stating that “the D.C. Circuit held that although plaintiffs had failed to establish a prima facie case of personal jurisdiction and the court was unable to tell whether jurisdictional discovery would assist GTE on this score, plaintiffs were entitled to pursue [discovery].”). In such cases, a party is entitled to pursue “precisely focused discovery aimed at addressing matters relating to personal jurisdiction.” *GTE New Media Services, Inc.*, 199 F.3d at 1351-52.

B. DISCUSSION

Amici argue that the plaintiffs have failed to demonstrate with sufficient specificity the basis for personal jurisdiction for each defendant. To be sure, such a showing is certainly required when parties are identified and named. The Court would then be able to evaluate personal jurisdiction defenses. The present situation, however, is different. Here, the plaintiffs have only limited information about the putative defendants, namely their IP addresses and information about the methodology used to engage in allegedly infringing activity. *See Id.* at 1352 (record before the court was “plainly inadequate” and “[j]urisdictional discovery will help to sort out these matters.”). Without additional information, the Court has no way to evaluate the defendants’ jurisdictional defenses. *See, e.g., London-Sire Records, Inc. v. Doe I*, 542 F. Supp. 2d 153, 180-181 (D. Mass. 2008) (“premature to adjudicate personal jurisdiction” and permitting plaintiff to engage in jurisdictional discovery); *Sony Music Entm’t, Inc. v. Does I-40*, 326 F. Supp. 2d 556, 567 (S.D.N.Y. 2004) (evaluating personal jurisdiction premature without defendants’ identifying information).

Amici contend that the plaintiffs do not have a “good faith” basis to assert personal jurisdiction over the putative defendants, and the Court should therefore not allow the defendants

to proceed with discovery. According to Amici, such a good faith basis could be established by reliance upon geolocation information embedded in each IP address. Specifically, Amici assert that IP addresses can be used to detect an individual's location and the plaintiffs should be forced to justify the putative defendants' personal jurisdiction by using tools "freely available to the public [that] help reveal where a person using a particular IP address is likely to be physically located." Amici Mem., at 5. Amici cite 'reverse domain name service lookup' ("reverse DNS") and the American Registry for Internet Numbers (the "ARIN database") as tools that would help reveal where a specific IP address is "likely to be physically located." Amici Mem., *Wild*, ECF No. 11, Seth Schoen Decl., at ¶¶ 5, 13.

The Court rejects this argument for three reasons. First, as the Amici concede, publicly available IP lookups reveal only where a defendant is "likely" to be located. *Id.* at ¶ 4. Given that these lookup tools are not completely accurate, this does not resolve the question of whether personal jurisdiction would be proper. Ultimately, the Court would still be unable to properly evaluate jurisdictional arguments until the putative defendants are properly identified and named. *See Sony*, 326 F. Supp. 2d. at 567-68 ("Assuming personal jurisdiction were proper to consider at this juncture, the [publicly available IP lookup] techniques suggested by amici, at best, suggest the mere 'likelihood' that a number of defendants are located [outside this jurisdiction]. This, however, does not resolve whether personal jurisdiction would be proper.").

Second, the nature of the BitTorrent technology enables every user of the file-sharing protocol to access copyrighted material from other peers, who may be located in multiple jurisdictions "around the country," including this one. Amended Compl., *Wild*, ECF No. 6, ¶ 4. Amici raise the prospect that the consequence of this theory is that any Internet user may be haled into court in any jurisdiction in the country for any online activity. Transcript of Mot.

Hearing at 34-35, *Call of the Wild Movie LLC v. Does 1-1,063*, No. 10-cv-455 (Mar. 1, 2011) (“If merely placing information online were enough to establish personal jurisdiction in the District or anyplace their information could be obtained and downloaded and accessed, the limits on personal jurisdiction would be abolished.”). While that broad prospect would indeed be troubling, that is not the situation here. *See generally GTE New Media Servs.*, 199 F.3d at 1350 (“[T]he advent of advanced technology, say, as with the Internet, should [not] vitiate long-held and inviolate principles of federal court jurisdiction.”). The allegations in the Complaints in *Wild*, *Maverick* and *Donkeyball* do not involve general Internet access, but specific use of a file-sharing protocol that may touch multiple jurisdictions to effectuate a download of a single copyrighted work. Moreover, so far, no putative defendant has been named or “haled” before this Court. The plaintiffs in each case will be able to proceed only against those named defendants over whom this Court has personal jurisdiction.

Finally, at this juncture when no putative defendant has been named, the Court has limited information to assess whether any putative defendant has a viable defense of lack of personal jurisdiction or to evaluate possible alternate bases to establish jurisdiction. *See, e.g., London-Sire Records, Inc.*, 542 F. Supp. 2d at 181 (“Even taking all of the facts in [the putative defendant’s] affidavit as true, it is possible that the Court properly has personal jurisdiction.”); *Humane Soc’y of the United States v. Amazon.com, Inc.*, No. 07-623, 2007 U.S. Dist. LEXIS 31810, at *10 (D.D.C. May 1, 2007) (“[A] plaintiff faced with a motion to dismiss for lack of personal jurisdiction is entitled to reasonable discovery, lest the defendant defeat the jurisdiction of a federal court by withholding information on its contacts with the forum,” quoting *Virgin Records Am., Inc. v. Does 1-35*, No. 05-1918, 2006 WL 1028956, at *3 (D.D.C. Apr. 18, 2006)). Certainly, the Court concurs with Amici that the putative defendants deserve to have dispositive

issues, such as personal jurisdiction, decided promptly. Amici Reply Brief, *Wild*, ECF No. 22, at 10. When the defendants are named, they will have the opportunity to file appropriate motions challenging the Court's jurisdiction and that will be the appropriate time to consider this issue. *See Virgin Records*, 2006 WL 1028956, at *3 (Amici's personal jurisdiction arguments rejected since "Defendant's Motion to Quash is without merit [] because it is premature to consider the question of personal jurisdiction in the context of a subpoena directed at determining the identity of the Defendant," citing *Elektra Entm't Grp., Inc. v. Does 1-9*, No. 04-2289, 2004 WL 2095581, at *5 (S.D.N.Y. Sept. 8, 2004); *Sony*, 326 F. Supp. 2d 556, 567-68 (S.D.N.Y.2004); *UMG Recordings v. Does 1-199*, No. 04-0093, at *2 (D.D.C. Mar. 10, 2004)).

The Court and parties are in no position yet to evaluate each putative defendant's specific connection with this jurisdiction. Quashing the subpoenas would effectively bar the plaintiffs' from obtaining discovery pertinent to that evaluation, and this Court declines to cut off jurisdictional discovery prematurely.

IV. THE PUTATIVE DEFENDANTS' FIRST AMENDMENT RIGHT TO ANONYMITY

Amici contend that the putative defendants' are entitled to First Amendment protection for their "anonymous communication." Amici Mem., at 14. Amici request, therefore, that the Court consider whether the First Amendment prevents disclosure of the defendants' identifying information and whether the plaintiffs have demonstrated a need to override that protection.⁵

Amici's request raises two questions for the Court to evaluate: First, are the putative defendants'

⁵ Amici also urge the Court to "set an example of what appropriate procedures must be followed before individuals' identities can be disclosed," including that notice be required to be sent to a customer before identifying information is provided in response to the subpoenas. Amici Mem., *Wild*, ECF No. 18, at 14-19. Such notices are already provided. Transcript of Mot. Hearing at 51, *Call of the Wild Movie LLC v. Does 1-1,063*, No. 10-cv-455 (Mar. 1, 2011) (plaintiffs' counsel: "Every single subpoena we sent to an ISP has [Amici's suggested] notice attached to it. And Time Warner, I believe, reached an agreement on the form of that notice . . . and every single subpoena we sent since that date in every new case has that notice.").

BitTorrent activities covered by the First Amendment right to engage in anonymous speech? Second, if the First Amendment protects BitTorrent activity, does the plaintiffs' need for the defendants' identifying information override that protection?

A. THE DEFENDANTS' RIGHT TO ENGAGE IN ANONYMOUS BITTORRENT ACTIVITY

The First Amendment protects an individual's right to anonymous speech, *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 341-42 (1995) ("The freedom to publish anonymously extends beyond the literary realm"), and this protection extends to anonymous speech on the Internet. *Reno v. ACLU*, 521 U.S. 844, 870 (1997) ("There is 'no basis for qualifying the level of First Amendment scrutiny that should be applied to [the Internet]"); accord, *Sinclair v. TubeSockTedD*, 596 F. Supp. 2d 128, 131 (D.D.C. 2009) ("Such rights to speak anonymously apply . . . to speech on the Internet."). Although the right to anonymity is "an important foundation of the right to speak freely," *London-Sire Records*, 542 F. Supp. 2d at 163, the right to free speech is not absolute, and certain classes of speech, such as defamation, libel, and obscenity, for example, are deemed to be beyond the purview of the First Amendment. See *Chaplinsky v. New Hampshire*, 315 U.S. 568, 571 (1942) (" . . . the right of free speech is not absolute at all times and under all circumstances. There are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which has never been thought to raise any Constitutional problem."); *Beauharnais v. Illinois*, 343 U.S. 250, 266 (1952) (libel); *Miller v. California*, 413 U.S. 15, 23 (1973) (obscenity). Copyright infringement is not protected by the First Amendment. See *Harper & Row Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 555-57, 560 (1985) (discussing copyright, the fair use doctrine, and the First Amendment). Amici argue, however, that the First Amendment protects "the anonymous publication of expressive works on the Internet even where, as here, the publication is alleged to infringe

copyrights.” Amici Mem., at 14. The question for this Court is whether the putative defendants are engaging in any expressive communication when they share files through BitTorrent that is entitled to some First Amendment protection of their anonymity.

While copyright infringement is not afforded First Amendment protection, file-sharing does involve aspects of expressive communication. *See Sony*, 326 F. Supp. 2d at 564 (“the file sharer may be expressing himself or herself through the music selected and made available to others.”); *see also London-Sire*, 542 F. Supp. 2d at 163 (“there are some creative aspects of downloading music or making it available to others to copy: the value judgment of what is worthy of being copied; the association of one recording with another by placing them together in the same library; the self-expressive act of identification with a particular recording; the affirmation of joining others listening to the same recording or expressing the same idea [W]hile the aspect of a file-sharer’s act that is infringing is not entitled to First Amendment protection, other aspects of it are.”). File-sharers, for example, indicate the artistic works they prefer when they decide to share or download a particular file. This expression can be noticed by other BitTorrent users and can indicate the relative popularity of particular files among a group of individuals.

File-sharers therefore do engage in expressive activity when they interact with other users on BitTorrent. The First Amendment interest implicated by their activity, however, is minimal given that file-sharers’ ultimate aim “is not to communicate a thought or convey an idea” but to obtain movies and music for free.⁶ *Sony*, 326 F. Supp. 2d at 564. Even if expression were an

⁶ Amici provide a declaration from Seth Schoen, in which Mr. Schoen states: “BitTorrent provides users with less ability to identify and communicate with the peers with whom they exchange files than other technologies do There is no easy way for the various BitTorrent users who have uploaded or downloaded parts of a file to recognize, name, or communicate with one another.” Amici Reply Brief, Seth Schoen Decl. in Support of Reply Brief ¶9, *Wild*, ECF No. 22. Although this information was supplied to support Amici’s contention that the putative defendants are improperly joined, it demonstrates rather that the putative defendants’ BitTorrent activities deserve

ancillary aim, the underlying method of the users' communication is illegal. This Court therefore joins a number of other jurisdictions who have deemed that a file sharer's First Amendment right to anonymity is "exceedingly small." *Arista Records LLC v. Does 1-19*, 551 F. Supp. 2d 1, 8 (D.D.C. 2008) ("First Amendment privacy interests are exceedingly small where the 'speech' is the alleged infringement of copyrights."); *see also Achte/Neunte Boll Kino Beteiligungs GMBH & Co, KG v. DOES 1-4*, 577, No. 10-453, 2010 U.S. Dist. LEXIS 94594, at *10 n.2 (D.D.C. Sept. 10, 2010) ("the protection afforded to such speech is limited and gives way in the face of a prima facie showing of copyright infringement"); *West Bay One, Inc. v. Does 1-1653*, 270 F.R.D. 13, 16 n.4 (D.D.C. July 2, 2010) (utilizing same language as *Achte/Neunte*, 2010 U.S. Dist. LEXIS 94594, at *10 n.2); *Sony*, 326 F. Supp. 2d at 567 (First Amendment right of alleged file-sharers to remain anonymous "must give way to the plaintiffs' right to use the judicial process to pursue what appear to be meritorious copyright infringement claims."); *Elektra Entm't Group, Inc. v. Does 1-9*, No. 04-2289, 2004 WL 2095581, at *4-5 (S.D.N.Y. Sept. 8, 2004) (finding that First Amendment right to anonymity overridden by plaintiff's right to protect copyright).

Nevertheless, file-sharers are engaged in expressive activity, on some level, when they share files on BitTorrent, and their First Amendment rights must be considered before the Court allows the plaintiffs to override the putative defendants' anonymity by compelling the production of these defendants' identifying information. *See Sony*, 326 F. Supp. 2d at 564 ("Although this is not political expression entitled to the broadest protection of the First Amendment, the file sharer's speech is still entitled to some level of First Amendment protection.") (internal quotations omitted).

even less First Amendment protection because BitTorrent allows for less communication between users than other file-sharing programs.

B. PLAINTIFFS' NEED TO OVERRIDE FIRST AMENDMENT PROTECTIONS AND IDENTIFY THE PUTATIVE DEFENDANTS

To assess whether the plaintiffs' subpoena should override the putative defendants' First Amendment rights, the Court uses the five-part test originally explicated in *Sony Music Entertainment v. Does 1-40*,⁷ 326 F. Supp. 2d at 564-65. This test has been applied by numerous courts across the country and in this district to similar file-sharing copyright infringement actions. *See, e.g., Arista Records*, 551 F. Supp. 2d at 8 (D.D.C. 2008) (Kollar-Kotelly, J.); *Achte/Neunte*, 2010 U.S. Dist. LEXIS 94594, at *10 n.2 (D.D.C. 2010) (Collyer, J.); *West Bay One*, 270 F.R.D. at 16 n.4 (D.D.C. 2010) (Collyer, J.); *London-Sire*, 542 F. Supp. 2d at 164 (D. Mass 2008); *Arista Records, LLC v. Doe 3*, 604 F.3d 110 (2d Cir. 2010); *Virgin Records v. Doe*, No. 5:08-cv-389, 2009 U.S. Dist. LEXIS 21701 (E.D.N.C. Mar. 16, 2009); *Elektra Entm't Group Inc. v. Does 1-9*, No. 04-cv-2289, 2004 WL 2095581, at *3-4 (S.D.N.Y. Sept. 8 2004). The *Sony* test calls for the court to assess whether the plaintiffs' need for identifying information outweighs the putative defendants' right to First Amendment anonymity by balancing: (1) the

⁷ Amici urge the Court to adopt a more rigorous five-part balancing test that was originally set forth in *Dendrite International v. Doe*, a New Jersey state case that required: "(1) that the plaintiff undertake to notify the anonymous posters that they are the subject of a subpoena seeking their identity; (2) that the plaintiff specify the exact statement alleged to constitute actionable speech; (3) that the court review the complaint and other information to determine whether a viable claim against the anonymous defendants is presented; (4) that the plaintiff produce sufficient evidence to support, prima facie, each element of its cause of action; and (5) that the court then balance the First Amendment right of anonymous speech against the strength of the plaintiff's prima facie claim and the need for disclosure of the anonymous defendant's identity." *Dendrite Int'l v. Doe*, 775 A.2d 756, 760-61 (N.J. Super. Ct. App. Div. 2001); *see also Sinclair v. TubeSockTedD*, 596 F. Supp. 2d 128 (D.D.C. 2009) (discussing, but not adopting the *Dendrite* test) (Bates, J.). The *Dendrite* test was applied in a defamation case; the case that discusses the *Dendrite* test in this district was also a defamation action. *Sinclair*, 596 F. Supp. 2d 128 (defamation action in which plaintiff sought identifying information for three anonymous online posters). This test has generally not been adopted in file-sharing cases. *See, e.g., London-Sire*, 542 F. Supp. 2d at 164 n.2 ("Dendrite, like many other cases involving internet speech, is not directly applicable to [file-sharing cases]. In that case, the plaintiff asserted that the anonymous defendant had defamed it on an internet bulletin board-an act much more clearly in the wheelhouse of the First Amendment's protections."); *Sony BMG Music Entm't v. Doe*, No. 5:08-109, 2009 WL 5252606, at *7 n.14 (E.D.N.C. Oct. 21, 2009) ("The protected speech at issue in *Dendrite* was allegedly defamatory comments posted on an internet bulletin, not the less expressive act of distributing music over the internet. In addition, the claim in *Dendrite* was for defamation, not copyright infringement, a unique area of particular federal concern."). The First Amendment interests implicated in defamation actions, where expressive communication is the key issue, is considerably greater than in file-sharing cases. The Court therefore believes that the *Sony* test is more applicable to the present case.

concreteness of the plaintiffs' showing of a prima facie claim of actionable harm; (2) the specificity of the plaintiffs' discovery request; (3) alternative means to get the information the plaintiffs seek; (4) the need for the information to advance the plaintiffs' claim; and (5) the objecting party's expectation of privacy. *Sony*, 326 F. Supp. 2d at 564-65.

1. Plaintiffs' Showing of a Prima Facie Claim

The first factor of the *Sony* analysis seeks to protect against gratuitous disclosure of identifying information when an individual's First Amendment anonymity rights are implicated. As one court noted, "people who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identity." *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999) (pre-dating the *Sony* test, but recognizing the difficulty facing courts when confronted with civil subpoenas seeking disclosure of identifying information for anonymous Internet users). To this end, courts must ensure that plaintiffs have made a "concrete" showing of a prima facie claim. *Sony*, 326 F. Supp. 2d at 565. For the plaintiffs to establish a prima facie claim of copyright infringement, they must demonstrate: (1) ownership of a valid copyright, and (2) copying of constituent elements of the work that are original. *Feist Pub'ns, Inc. v. Rural Tel. Serv. Co., Inc.*, 499 U.S. 340, 361 (1991).

Plaintiffs have adequately demonstrated a prima facie claim of copyright infringement against the putative defendants. First, the plaintiffs allege that they are "holder[s] of the pertinent exclusive rights infringed by Defendants" and cite to certificates of copyrights issued by the Registrar of Copyrights. Amended Compl., *Wild*, ¶ 10; *see also* Amended Compl. *Maverick*, ¶ 9; Compl., *Donkeyball*, No. 10-1520, ¶ 10. The plaintiffs further assert that the putative defendants violated the plaintiffs' exclusive rights of reproduction and distribution when

they, “without the permission or consent of Plaintiff[s], distributed the Copyrighted Motion Picture[s] to the public, including by making available for distribution to others.” *Id.* at ¶ 12.

The plaintiffs support these allegations by supplying the date and time that the alleged infringement occurred, along with affidavits from Messrs. Benjamin Perino and Patrick Achache describing the process by which the defendants’ infringement was observed, recorded, and verified.⁸ Pl.’s Mot. for Leave to Take Disc. Prior to Rule 26(f) Conference, *Wild*, ECF No. 2, Benjamin Perino Decl., Patrick Achache Decl.; Pl.’s Mot. for Leave to Take Disc. Prior to Rule 26(f) Conference, *Maverick*, ECF Nos. 4-6, Benjamin Perino Decl., Patrick Achache Decl.; Pl.’s Mot. for Leave to Take Disc. Prior to Rule 26(f) Conference, *Donkeyball*, ECF No. 4, Benjamin Perino Decl., Patrick Achache Decl. Accordingly, the plaintiffs have appropriately pled a prima facie claim of copyright infringement against the putative defendants.

2. The Specificity of the Plaintiffs’ Discovery Requests

The second *Sony* factor weighs the specificity of the plaintiffs’ requests for identifying information. This factor is intended to keep the plaintiffs’ request narrow so as to prevent overbroad discovery requests that “unreasonably invade[] the anonymity of users who are not alleged to have infringed” *London-Sires*, 542 F. Supp. 2d. at 178. In *Wild*, *Maverick*, and *Donkeyball*, the Court granted the plaintiffs leave to subpoena ISPs for the putative defendants’ name, current and permanent address, telephone number, e-mail address, and Media Access

⁸ During oral argument, Amici noted that the declarations of Messrs. Perino and Achache submitted by plaintiffs in support of their motions for leave to take expedited discovery in *Wild* and *Maverick* are dated December 31, 2009, even though a number of the putative defendants are alleged to have engaged in infringing activity after that date. Transcript of Mot. Hearing, at 46-47, Call of the Wild Movie LLC v. Does 1-1,063, No. 10-cv-455 (Mar. 1, 2011); see also Pl.’s Mot. Leave to Take Expedited Disc., *Maverick*, ECF No. 4, Benjamin Perino Decl., ¶ 11; Pl.’s Mot. Leave to Take Expedited Disc., *Donkeyball*, ECF No. 4, Benjamin Perino Decl., ¶ 11. These declarations only purport to describe the procedures used to identify those accused of illegally distributing plaintiffs’ motion pictures and, thus, the date of that description does not undercut the claims against the putative defendants, as Amici appear to imply.

Control address. Order Granting Pl.'s Mot. Expedited Discovery, at 2, *Wild*, Apr. 15, 2010, ECF No. 4; Order Granting Pl. Mot. Expedited Discovery, *Maverick*, May, 24 2010, ECF No. 7;; Order Granting Expedited Discovery, *Donkeyball*, Oct. 19, 2010, ECF No. 6. This information will enable the plaintiffs to properly name and serve the putative defendants. By court order, this information "may be used by the plaintiff solely for the purpose of protecting the plaintiff's rights as set forth in the complaint." *Id.* These limited discovery requests, along with the restrictions imposed by the Court, are specifically targeted to obtain the information plaintiffs need to prosecute their lawsuits.

3. No Alternate Means to Obtain the Information

The third *Sony* factor inquires whether the plaintiffs have any other means to obtain the defendants' identifying information other than compelling the information from ISPs. The plaintiffs state that without expedited discovery the "Plaintiff[s] ha[ve] no way of serving Defendants with the complaint and summons in this case. Plaintiff[s] do[] not have Defendants' names, addresses, e-mail addresses, or any other way to identify or locate Defendants, other than the unique IP address assigned to each Defendant by his/her ISP on the date and at the time of the Defendant's infringing activity." Pl.'s Mot. for Leave to Take Disc. Prior to Rule 26(f) Conference, *Wild*, ECF No. 2, Benjamin Perino Decl., ¶ 11. Amici and Time Warner do not dispute that the plaintiffs have no other sources for the information they seek.

4. Plaintiffs' Need for the Information

The plaintiffs have sufficiently alleged prima facie claims of copyright infringement against the putative defendants, and have also demonstrated that there are no alternate means to obtain the defendants' identifying information. Without this information from the ISPs, the plaintiffs cannot name and serve those whom they allege to have infringed upon their copyrights.

Pl.'s Mot. for Leave to Take Disc. Prior to Rule 26(f) Conference, *Wild*, ECF No. 2, Benjamin Perino Decl., ¶ 11. (“Without expedited discovery . . . Plaintiff[s] [have] no way of serving Defendants with the complaint and summons in this case.”). The putative defendants’ identifying information is therefore critical to the plaintiffs’ cases.

5. The Putative Defendants’ Expectation of Privacy

As previously discussed, the putative defendants have minimal First Amendment protection against disclosure of their identities in the face of the plaintiffs’ allegations that they infringed the plaintiffs’ copyrights. Their expectation of privacy is similarly minimal in this context.

This conclusion is underscored by Time Warner’s Terms of Service, which specifically warns customers against engaging in illegal infringing activity, with the penalty of termination or suspension of service:

“Time Warner Cable’s subscribers and account holders may not upload, post, transmit or otherwise make available on or via the Road Runner Service any material protected by copyright in a manner that infringes that copyright. In accord with the Digital Millennium Copyright Act, it is the policy of Time Warner Cable to terminate in appropriate circumstances the Road Runner Service of any subscriber or account holder who is a repeat infringer. . . . Time Warner Cable expressly reserves the right to terminate or suspend the service of any subscriber or account holder even for a single act of infringement.”

Time Warner’s Reply to Pl.’s Opposition to Time Warner’s Mot. Quash, *Donkeyball*, ECF No. 16, at 8 n.2.

Further, available on Time Warner’s website is the Time Warner Cable Subscriber Privacy Notice, which is provided to users “upon initiation of service and annually thereafter.” TIME WARNER CABLE SUBSCRIBER PRIVACY NOTICE (July 2010), *available at* http://help.twcable.com/html/twc_privacy_notice.html. This notice informs customers that Federal law requires Time Warner to “disclose personally identifiable information to a governmental entity

or other third parties pursuant to certain legal process . . . [Time Warner] will comply with legal process when we believe in our discretion that we are required to do so. We will also disclose any information in our possession to protect our rights, property and/or operations, or where circumstances suggest that individual or public safety is in peril.” *Id.*

Time Warner informed its customers that it was monitoring for instances of copyright infringement, and if a customer did engage in such conduct, Time Warner would likely terminate or suspend the customer’s service. Time Warner’s privacy notice also explicitly informs customers that their information could be disclosed upon court order. Thus, under these circumstances, the putative defendants have little to no expectation of privacy while engaging in allegedly infringing activities about which they are warned against. *See generally Sony*, 326 F. Supp. 2d at 566-67 (minimal expectation of privacy when ISP’s terms of service prohibit copyright infringement and state that information can be relayed to law enforcement).

C. DEFENDANTS’ FIRST AMENDMENT RIGHTS DO NOT PREVENT DISCLOSURE OF IDENTIFYING INFORMATION

Upon balancing the putative defendants’ First Amendment rights to anonymity and the plaintiffs’ need for the identifying information, the Court finds that the plaintiffs’ need overrides the putative defendants’ right to use BitTorrent anonymously. The putative defendants’ asserted First Amendment right to anonymity in this context does not shield them from allegations of copyright infringement. The plaintiffs therefore may obtain from ISPs information identifying the putative defendants.

V. TIME WARNER’S MOTION TO QUASH

Having considered the arguments put forth by Amici in support of Time Warner’s Motion to Quash, the Court turns to Time Warner’s own arguments to quash the plaintiffs’

subpoenas pursuant to Federal Rule of Civil Procedure 45(c). Time Warner argues that producing the requested information would subject it to an undue burden and, if the subpoenas are not quashed, seeks to modify the subpoenas to limit Time Warner's compliance to production of identifying information for 28 IP addresses per month.⁹ For the reasons discussed below, Time Warner has failed to demonstrate that the burdens associated with producing the requested information justify quashing the plaintiffs' subpoenas or limiting Time Warner's production obligations.

A. LEGAL STANDARD

Pursuant to Federal Rule of Civil Procedure 45, the Court must quash a subpoena issued to a nonparty if the subpoena subjects the nonparty to an undue burden or expense. FED. R. CIV. P. 45(c). The nonparty seeking relief from subpoena compliance bears the burden of demonstrating that a subpoena should be modified or quashed. *See Linder v. Dep't of Defense*, 133 F.3d 17, 24 (D.C. Cir. 1998); *In re Micron Technology Inc. Securities Lit.*, 264 F.R.D. 7, 9 (D.D.C. 2010); *Achte/Neunte*, 736 F. Supp. 2d 212, 215 (D.D.C. 2010).

Quashing subpoenas "goes against courts' general preference for a broad scope of discovery, [but] limiting discovery is appropriate when the burden of providing the documents outweighs the need for it." *North Carolina Right to Life, Inc. v. Leake*, 231 F.R.D. 49, 51 (D.D.C. 2005) (internal citations omitted). When evaluating whether the burden of subpoena compliance is "undue," the court balances the burden imposed on the party subject to the subpoena by the discovery request, the relevance of the information sought to the claims or

⁹ Time Warner notes that another judge in this district also denied Time Warner's motions to quash in two file-sharing cases, but granted a protective order limiting Time Warner's subpoena production obligations in those cases to only 28 IP addresses a month. *See Achte/Neunte Boll Kino Beteiligungs GMBH & Co, KG v. Does 1 - 4,577*, No. 10-cv-00453, ECF No. 33 (D.D.C. July 2, 2010) (Collyer, J.); *West Bay One, Inc. v. Does 1-1653*, No. 10-cv-00481, ECF No. 24 (D.D.C. July 2, 2010) (Collyer, J.). This Court is not bound by findings in other cases and, in any event, this Court evaluated information not directly considered by the other court, including Time Warner's efforts to preserve the requested information, and supplemental affidavits from plaintiffs, Time Warner, and Amici.

defenses at issue, the breadth of the discovery request, and the litigant's need for the information. *See id.* at 51; *Linder*, 133 F.3d at 24 (“Whether a burdensome subpoena is reasonable must be determined according to the facts of the case, such as the party's need for the documents and the nature and importance of the litigation.”) (internal quotations omitted); *Achte/Neunte*, 736 F. Supp. 2d at 214. The court must limit discovery when the “burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties’ resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.” FED. R. CIV. P. 26(b)(2)(C)(iii). The ‘undue burden’ test also requires the court to be “generally sensitive to the costs imposed on third-parties.” *In re Micron Tech.*, 264 F.R.D. at 9.

B. EVALUATING TIME WARNER’S BURDEN

At the outset, Time Warner does not dispute that the identifying information sought by the subpoenas is critical to the plaintiffs’ lawsuits since without production of this information, the plaintiffs are unable to name and serve the putative defendants. In addition, Time Warner does not claim that the subpoenas seek any more information than the Court authorized: namely, “information sufficient to identify each defendant, including his or her name, current and permanent address(es), telephone number(s), e-mail address(es), and Media Access Control address(es).” Order Granting Expedited Disc., *Wild*, ECF No. 4, Apr. 15, 2010; Order Granting Expedited Disc., *Maverick*, ECF No. 7, May, 24 2010; Order Granting Expedited Disc., *Donkeyball*, ECF No. 6, Oct. 19, 2010. Thus, the plaintiffs’ requests are not unspecific, undefined or unduly broad. *Cf. North Carolina Right to Life*, 231 F.R.D. at 52 (quashing subpoena in part because discovery request sought “vast array of documents arising from ‘contacts’” between parties).

Nevertheless, Time Warner characterizes plaintiffs' discovery demands as "overbroad." Time Warner Mem. Supp. Mot. Quash, *Wild*, at 12. The respective plaintiffs in these three cases subpoenaed Time Warner for information relating to a total of 1,028 IP addresses. Time Warner Mot. Quash, *Wild*, ECF No. 7, Ex. 1 (224 IP addresses); Time Warner Mot. Quash, *Maverick*, ECF No. 18, Ex. 1 (783 IP addresses); Time Warner Mot. Quash, *Donkeyball*, ECF No. 7, Ex. 1 (21 IP addresses). The overbreadth that Time Warner complains of is due to the large number of Time Warner's customers allegedly engaging in infringing activities and prompting the plaintiffs' need for their identifying information. This, however, does not render the subpoenas overbroad in terms of the information requested about each defendant.

Thus, Time Warner's principle contention is that, due to the large number of its customers allegedly engaging in online infringing activities, it would "suffer significant harms" and "incur significant costs" because compliance with requests for identifying information about those customers would "overwhelm" its capacity and "completely absorb the resources for many months." Time Warner Mot. Quash, *Donkeyball*, ECF No. 7, Ex. 2, Craig Goldberg Aff. dated Dec. 10, 2010, ¶¶ 9,12; *see also* Time Warner Mot. Quash, *Maverick*, ECF No. 18, Craig Goldberg Aff. dated Nov. 22, 2010, ¶¶ 9,12; Time Warner Mot. Quash, *Wild*, ECF No. 7, Craig Goldberg Aff. dated May 10, 2010, ¶¶ 7, 9. To support its motions, Time Warner initially submitted a single four-page affidavit by Craig Goldberg, Assistant Chief Counsel, Litigation and Time Warner's Chief Privacy Officer, in all three cases. This affidavit provided general and conclusory information about the Time Warner subpoena compliance process. Following oral argument on Time Warner's motions to quash, the company supplemented the record with an

additional affidavit.¹⁰ Notwithstanding the supplemental affidavit, Time Warner has failed to demonstrate that complying with the plaintiffs' subpoenas would subject it to an undue burden.

Time Warner describes its subpoena compliance operations as follows: Within its legal department, Time Warner has a "subpoena compliance team" comprised of five full-time employees and one temporary employee who focus "exclusively" on responding to subpoena requests, court orders, and National Security Letters. Time Warner Mot. Quash, *Donkeyball*, ECF No. 7, Goldberg Aff. dated Dec. 10, 2010, at ¶ 3; *see also* Time Warner Mot. Quash, *Maverick*, ECF No. 18, Craig Goldberg Aff. dated Nov. 22, 2010; Time Warner Mot. Quash, *Wild*, ECF No. 7, Craig Goldberg Aff. dated May 10, 2010. In both its unsealed and sealed affidavits, Time Warner indicates that it received approximately 567 IP lookup requests a month, mostly from law enforcement, but does not specify over what period of time this was the average number.¹¹ *Id.* at ¶ 6. In both affidavits Time Warner also contends that it cannot divert any more resources toward responding to subpoena requests "without harming its efforts to assist law enforcement and overburdening [Time Warner's] subpoena response team." *Id.* at ¶ 8. Time Warner complains that, from February to December 2010, Time Warner "received over two

¹⁰ Time Warner moved for, and the Court granted, leave to file a supplemental affidavit under seal because Time Warner represented that the supplemental affidavit relayed "highly proprietary" and "competitively sensitive information the disclosure of which could harm TWC's business interests," and prejudice both TWC and law enforcement. Time Warner's Mot. for Leave to File Affidavit Under Seal, *Wild*, ECF No. 38, March 17, 2011; Minute Order, *Wild*, March 22, 2011 (granting leave to file affidavit under seal); Time Warner's Mot. for Leave to File Affidavit Under Seal, *Maverick*, ECF No. 45, March 17, 2011; Minute Order, *Maverick*, March 17, 2011 (granting leave to file affidavit under seal); Time Warner's Mot. for Leave to File Affidavit Under Seal, *Donkeyball*, ECF No. 23, March 17, 2011; Minute Order, *Donkeyball*, March 17, 2011 (granting leave to file affidavit under seal). The sealed, supplemental affidavit contains certain information already provided to the Court in the initial, public affidavit, and the Court is hard-pressed to understand why the names of commercially available software and hardware equipment and tools used by Time Warner warrant sealing. Therefore, the Court will order Time Warner to review the sealed, supplemental affidavit and to file publicly a version from which Time Warner has redacted only the information that reflects clearly proprietary and security sensitive information. For each item redacted, Time Warner is required to provide the Court with an explanation specifying what makes the redacted information "proprietary" or "security sensitive."

¹¹ Time Warner states this was the average number of IP lookup requests "[p]rior to requests associated with file-sharing litigation." Without more specific information about the time period, it is unclear whether that was the average number over the past year, the past five years, or some other time period.

dozen subpoenas” for 4,100 IP lookups in file-sharing cases from “private litigants,” *id.* at ¶ 7, but provides no information about how many of these subpoenas originated from the plaintiffs or plaintiffs’ counsel.

Time Warner states that producing the information requested by the plaintiffs is a “multi-step process” that “requires both centralized efforts at [Time Warner]’s corporate offices, as well as efforts at the local operations center where the relevant subscriber is located.” *Id.* at ¶ 5. This “multi-step process” is not unusual. Most consumer IP addresses are ‘dynamic’ as opposed to ‘static.’ *See generally London-Sires*, 542 F. Supp. 2d at 160. Static IP addresses are addresses which remain set for a specific user. *Id.* Dynamic IP addresses are randomly assigned to internet users and change frequently. *Id.* Consequently, for dynamic IP addresses, a single IP address may be re-assigned to many different computers in a short period of time. *Id.*

Associating a dynamic IP address with a particular customer at a given moment makes the task of “discovering the identity of a particular infringer more difficult.” *Id.*; *see also U.S. v. Steiger*, 318 F.3d 1039, 1042 (11th Cir. 2003)(“Static addresses are undoubtedly easier to trace, but ISPs generally log the assignments of their dynamic addresses.”). This requires ISPs to maintain logs and other records, and to use commercially available or customized software tools, to correlate the IP address assigned to a computer at a specific moment with the subscriber’s account information in order to identify a customer from the IP address, either for the ISPs own internal business purposes or to respond to subpoenas requesting identifying information about a customer. *See, e.g., Klimas v. Comcast Cable Commc’n, Inc.*, 465 F.3d 271, 275 (6th Cir. 2006)(“dynamic IP addresses constantly change and unless an IP address is correlated to some other information, such as Comcast’s log of IP addresses assigned to its subscribers..., it does not identify any single subscriber by itself.”)(internal quotations omitted);

Time Warner describes the process as “time consuming and can require the work of multiple people at multiple locations.” Time Warner Mot. Quash, *Donkeyball*, ECF No. 7, Ex. 2, Craig Goldberg Aff. at ¶5. This information, even when supplemented by Time Warner’s sealed affidavit, does not support Time Warner’s contention that compliance with the plaintiffs’ subpoenas in *Wild*, *Maverick*, and *Donkeyball* subject it to an undue burden. Time Warner concedes that in order to pursue its motions to quash it has already taken steps to isolate and preserve the information necessary to provide customer identifying information for the requested IP addresses. See Transcript of Mot. Hearing at 9, *Call of the Wild Movie LLC v. Does 1-1,063*, No. 10-cv-455 (Mar. 1, 2011) (Time Warner’s counsel states that its client has “incurred a substantial burden already” by preserving the data.). It has been eleven months since Time Warner was issued a subpoena in *Wild*, six months since the subpoena in *Maverick* was issued, and four months since the subpoena in *Donkeyball* was issued. Time Warner’s Mot. Quash, *Wild*, ECF No. 7, Ex. 1, Subpoena dated April 30, 2010; Time Warner’s Mot. Quash, *Maverick*, ECF No. 18, Ex. 1, Subpoena dated Sept. 14, 2010; Time Warner’s Mot. Quash, *Donkeyball*, ECF No. 7, Ex. 1, Subpoena dated Nov. 11, 2010. In this timeframe, Time Warner accomplished “fifty-percent or more” of the work necessary to respond to the subpoenas by isolating and preserving the data. Transcript of Mot. Hearing, at 12, *Call of the Wild Movie LLC v. Does 1-1,063*, No. 10-cv-455 (Mar. 1, 2011) (Time Warner’s counsel stating that “something on the order of, you know, 50 percent or more [of the work] may have already been done”). If it took less than one year to complete fifty percent of the work, it is difficult to see why it will take over three more years, at 28 IP address lookups per month, to complete the production.

Time Warner’s contention that it can only produce 28 IP addresses per month seems extraordinarily dilatory compared to the rate at which other ISPs are able to produce the

requested information. *See* Supplemental Declaration of Nicholas Kurtz, *Maverick*, ECF No. 42, ¶ 6 (relaying that in *Achte*, No. 10-cv-453 (D.D.C.) (Collyer, J.) and *West Bay One*, No. 10-cv-481 (D.D.C.) (Collyer, J.) Comcast averaged 141 IP lookups a month, Charter averaged 199 IP lookups a month, Cox averaged 113.43 IP lookups a month, and Verizon averaged 294.5 IP lookups a month). Time Warner's description of its "multi-step" process indicates that, in addition to the five-person subpoena compliance team, employees in its regional offices are able to assist in the process of identifying the customers associated with particular IP addresses. This suggests that when confronted with a large volume of subpoenas for identifying information about its customers that may strain its subpoena compliance team, Time Warner has additional resources already on staff in regional offices to address the production.

In addition, as part of the effort to resolve this discovery dispute without judicial intervention, the plaintiffs' counsel offered to pay Time Warner to employ another temporary worker to help respond to the plaintiffs' subpoena requests. Transcript of Mot. Hearing at 64, *Call of the Wild Movie LLC v. Does 1-1,063*, No. 10-cv-455 (Mar. 1, 2011) (plaintiffs' counsel states: "As a quick aside, in prior negotiations, we have offered to basically pay for a temporary employee. We have paid for the production, even though I argue -- and I think it is legitimate -- that we arguably don't have to pay for these productions because it is already part of their business."). Time Warner already employs a temporary worker to handle the volume of subpoena requests it must process as part of its business operations. Thus, while the company is under no obligation to accept this offer to defray costs, use of another temporary worker is not an extraordinary or unusual solution but instead consistent with its normal business practice to facilitate timely compliance with subpoenas.

Time Warner included with its general description of the subpoena compliance process a summary statement that the cost of producing identifying information for one IP address is \$45. Time Warner Mot. Quash, *Donkeyball*, ECF No. 7, Ex. 2, Craig Goldberg Aff. at ¶ 11. The study underlying this cost estimate contains no detail about the process used for subpoena compliance, but only general numbers regarding total employee compensation and alleged time spent responding to IP lookup requests. Pl.'s Opposition Time Warner's Mot. Quash, *Wild*, ECF No. 9, Ex. 2. Based on this estimate, the total cost to produce information in *Wild* would be "approximately \$10,080," Time Warner Mem. Supp. Mot. Quash, *Wild*, ECF No. 7, at 9, and in *Maverick* and *Donkeyball* approximately "\$36,180 (804 IP x \$45 IP addresses), plus the costs of notifying each subscriber." Time Warner Mem. Supp. Mot. Quash, *Donkeyball*, ECF No. 7, at 9-10.

When granting the plaintiffs leave to subpoena ISPs, the Court allowed the ISPs to charge the plaintiffs for the costs of producing the requested information. Order Granting Pl.'s Mot. for Expedited Discovery, *Wild*, ECF No. 4, April 15, 2010, at 3-4 ("ORDERED that any ISP that receives a subpoena and elects to charge for the costs of production shall provide a billing summary and any cost reports that serve as a basis for such billing summary and any costs claimed by such ISP . . ."); Order Granting Pl.'s Mot. for Expedited Discovery, *Maverick*, ECF No. 7, May 24, 2010, at 3 ("ORDERED that any ISP which receives a subpoena and elects to charge for the costs of production shall provide a billing summary and any cost reports that serve as a basis for such billing summary and any costs claimed by such ISP. . ."); *See also* Order Granting Pl.'s Mot. for Expedited Discovery, *Donkeyball*, ECF No. 6, Oct. 19, 2010 (not specifically mentioning billing provision, but see Pl.'s Mot. for Expedited Discovery, *Donkeyball*, ECF No. 4, Ex. 3, Text of Proposed Order, at 2). In so far as Time Warner argues

that cost alone serves as a basis to quash plaintiffs' subpoenas, that position is unavailing since the plaintiffs will cover the cost, per the court order.

Time Warner has failed to demonstrate that compliance with the plaintiffs' subpoena requests would impose an undue burden. Although Time Warner asserts that producing the requested information is a "multi-step process," it admits that "more than fifty percent" of the work has already been done, with the identifying information subject to the subpoena isolated and preserved. The Court sees no reason why Time Warner cannot expeditiously complete the processing of this information for production to the plaintiffs.

Time Warner's motions to quash in *Wild*, *Maverick*, and *Donkeyball* on the basis that the subpoenas are unduly burdensome are therefore denied.

C. TIME WARNER'S ALTERNATE ARGUMENTS TO QUASH PLAINTIFFS' SUBPOENAS

In *Wild* and *Maverick*, Time Warner proffers additional arguments to quash the plaintiffs' subpoenas. In *Wild*, Time Warner (1) asserts that plaintiffs' counsel breached an agreement that limited subpoena requests to 28 IP addresses a month, and (2) requests the Court to alter the parties' costs arrangement so as to order the plaintiff to pay Time Warner in advance of producing the requested information. Time Warner Mem. Supp. Mot. Quash, *Wild*, ECF No. 7, at 8, 11-12. In *Maverick*, Time Warner contends that the plaintiff did not properly serve Time Warner with its subpoena. Time Warner Mem. Supp. Mot. Quash, *Maverick*, ECF No. 18, at 15-17.

Time Warner has failed to demonstrate that the plaintiffs' subpoenas should be quashed in *Wild*. In *Wild*, there was no meeting of the minds between plaintiffs' counsel and Time Warner; and the Court additionally declines to alter the cost arrangement previously ordered by the Court. In *Maverick*, however, the plaintiff did not abide by the Federal Rules of Civil

Procedure when serving its subpoena. Time Warner's Motion to Quash in *Maverick* is therefore granted.

1. Purported Agreement to Limit Production in Wild

The Court first dispenses with Time Warner's argument that the Court should quash the plaintiff's subpoena in *Wild* because of a purported agreement with plaintiff's counsel to limit Time Warner's subpoena production to 28 IP addresses a month. In the District of Columbia, a valid contract requires "both (1) agreement as to all material terms; and (2) intention of the parties to be bound." *T Street Development, LLC v. Dereje and Dereje*, 586 F.3d 6, 11 (D.C. Cir. 2009). The Court primarily looks to intent of the parties entering into the agreement. *Christacos v. Blackie's House of Beef, Inc.*, 583 A.2d 191, 194 (D.C. 1990). Intent is an objective inquiry that the Court assesses by asking "what a reasonable person in the position of the parties would have thought the disputed language meant." *Id.* (quoting *1010 Potomac Assocs. v. Grocery Mfrs. of Am., Inc.*, 485 A.2d 199, 205 (D.C.1984)). The burden of proof that a contract exists falls on the party attempting to enforce the agreement. *See Novecon Ltd. v. Bulgarian-American Enterp. Fund*, 190 F.3d 556 (D.C. Cir. 1999).

Time Warner argues that it reached a "negotiated agreement" with plaintiffs' counsel that Time Warner would provide the plaintiff with information for 28 IP addresses a month "with the specific acknowledgement that it applied to all future subpoenas that [plaintiffs' counsel] served on [Time Warner]." Time Warner Mem. Supp. Mot. Quash, *Wild*, at 8. This agreement was not memorialized in a signed document, but rather, according to Time Warner, was negotiated and agreed to in string of emails dated March 19, 2010 discussing subpoena production in other file-sharing cases. Time Warner's Mot. Quash, *Wild*, ECF No. 7, Ex. 3. The Court has reviewed the emails cited by Time Warner and finds that there was no meeting of the minds and no evidence

that plaintiff's counsel agreed to limit Time Warner's obligations under the subpoenas to production of 28 IP addresses a month for all his clients, present and future. On the contrary, the last email sent by plaintiff's counsel Thomas Dunlap makes clear that he anticipated additional requests for IP lookups. *Id.*, Ex. 3 (email from Thomas M. Dunlap to Craig Goldberg Re: Subpoenas to TWC, dated March 19, 2010, 3:47 PM states: "[w]e may need to request more subpoenas, however we will discuss this with you before we send it over so we can work out a timetable and method.") Time Warner's contention that a prior agreement limits Time Warner's subpoena compliance obligations in *Wild* is therefore unsuccessful.

2. Cost-Shifting in *Wild*

In *Wild*, Time Warner requests that the Court alter the cost arrangement set forth in the Court's April 15, 2010 order, in which the Court granted the plaintiff leave to subpoena ISPs for identifying information regarding the putative defendants. Order Granting the Plaintiff's Mot. for Expedited Discovery, *Wild*, ECF No. 4. In that Order, the Court specifically stated that:

"... any ISP that receives a subpoena pursuant to this Memorandum Order shall *not assess any charge to the plaintiff before providing the information* requested in the Rule 45 subpoena, nor shall the ISP assess a charge to the plaintiff in connection with IP addresses that are not controlled by that ISP, *duplicate IP addresses that resolve to the same individual*, other IP addresses that do not provide the name and other information requested of a unique individual or for the ISP's internal costs incurred to notify the ISP's customers; and it is

ORDERED that any ISP that receives a subpoena and elects to charge for the costs of production shall provide a billing summary and any cost reports that serve as a basis for such billing summary and any costs claimed by such ISP . . ."

Id. at 3-4 (emphasis supplied). Time Warner now requests that the Court alter that arrangement so that Time Warner is paid in advance of providing the requested information to the plaintiff, and is paid "on a per-IP-address basis, rather than per subscriber." Time Warner Mem. Supp. Mot. Quash, *Wild*, at 11-12. Time Warner has proffered no complaints about plaintiffs' inability

or refusal to pay for subpoena compliance that would justify alteration of the order to a pre-payment plan. Nor does Time Warner contend that it is under such a financial hardship that pre-payment is required.

No other ISP subpoenaed by the plaintiff in *Wild* has come forward requesting that the order to be modified on grounds that this cost arrangement is unfair and the Court declines to make an exception for Time Warner, particularly given the paucity of the reasons proffered for the requested changes.

3. Improper Service of the Plaintiff's Subpoena in Maverick

As an alternate basis to quash the plaintiff's subpoena in *Maverick*, Time Warner asserts that the plaintiff did not serve its subpoena in accordance with Rule 45(b) of the Federal Rules of Civil Procedure. Specifically, Time Warner asserts that the plaintiff faxed and emailed Time Warner the *Maverick* subpoena, but never delivered the subpoena to a named person.

Under Federal Rule of Civil Procedure 45(b), "serving a subpoena requires delivering a copy to the named person." The "longstanding interpretation of Rule 45 has been that personal service of subpoenas is required. The use of the word "delivering" in subdivision (b)(1) of the rule with reference to the person to be served has been construed literally." 9A Charles Alan Wright & Arthur R. Miller, *Federal Practice and Procedure* § 2454 (2010). A minority of courts have broadened the interpretation of Rule 45(b) and held that personal in-hand service is not required. *See, e.g., Hall v. Sullivan*, 229 F.R.D. 501, 506 (D. Md. 2005) ("no reason to require in-hand delivery of subpoenas [*duces tecum*]-so long as the service is in a manner that reasonably ensures actual receipt of the subpoena by the witness."). Courts in this jurisdiction have not followed this path. *See, e.g., U.S. v. Philip Morris Inc.*, 312 F. Supp. 2d 27, 36-37 (D.D.C. 2004) (stating that "FED. R. CIV. P. 45(b) (1) requires personal service of deposition

subpoenas” and quashing subpoenas left in the party’s mail room); *Alexander v. F.B.I.*, 186 F.R.D. 128, 130 (D.D.C. 1998) (stating that it is “well settled that, under FED. R. CIV. P. 45(b), [the non-party’s] deposition subpoena must have been personally served upon him”).

It is undisputed that in *Maverick* plaintiff’s counsel forwarded the subpoena as an attachment to an email to Time Warner’s counsel on September 14, 2010. Pl.’s Opp’n To Time Warner Mot. Quash, ECF No. 22, Ex. 1 (email from Nicholas Kurtz to Alexander Maltas dated Sept. 14, 2010, 3:53 PM). In the text of the email, plaintiff’s counsel asked Time Warner’s counsel to accept service by email of the plaintiff’s subpoena. *Id.* The following day, Time Warner’s counsel responded via email that he was not authorized to accept such service. Time Warner’s Mot. Quash, *Maverick*, ECF No. 18, Ex. 5 (Letter from Alexander Maltas to Thomas Dunlap and Nicholas Kurtz dated October 13, 2010). Despite this disavowal of service, a week later, on September 22, 2010, a Time Warner representative named “Tammi” called plaintiff’s counsel and told him that she would be working on the subpoena and requested that he email a copy to her. Pl.’s Opp’n Time Warner’s Mot. Quash, *Maverick*, ECF No. 22, Nicholas Kurtz Decl., ¶ 4 and Ex. 2 (Kurtz email to ‘subpoena.compliance@twccable.com’ dated Sept. 22, 2010: “Pursuant to my telephone conversation with Tammi, attached is the Excel spreadsheet for the *Maverick* civil subpoena. I have also attached a PDF of the subpoena for your convenience.”). On October 13, 2010, Time Warner sent the plaintiff a letter stating that Time Warner had yet to be properly served with plaintiff’s subpoena in *Maverick*. Time Warner’s Mot. Quash, *Maverick*, ECF No. 18, Ex. 5 (Letter from Alexander Maltas to Thomas Dunlap and Nicholas Kurtz, dated October 13, 2010). Nevertheless, the plaintiff did not take steps to deliver the subpoena personally and relied solely upon service by fax and email.¹²

¹² Plaintiff argues that Time Warner’s “own subpoena compliance website states that [Time Warner] ‘accepts lawful process by fax.’” Pl.’s Mem. Opp’n Time Warner’s Mot. Quash, *Maverick*, ECF No. 22, at 16; Kurtz Decl., Ex. 6

The Federal Rules of Civil Procedure requires personal service of subpoenas. *See* FED. R. CIV. P. 45(b) (1). The Court acknowledges that strict adherence to the literal interpretation of Rule 45(b)(1) may place form over substance, particularly when, as here, the subpoenaed party acknowledges that it received the subpoena at issue and has a history of multiple contacts over subpoena compliance with the sender of the subpoena. At the same time, however, the plaintiff is required to comply with Rule 45(b) (1).

In a last gasp effort to avoid the quashing of the subpoena in *Maverick*, plaintiff's counsel argues -- without citation to any legal authority for this waiver argument -- that Time Warner's filing of the instant motion constitutes a waiver of its jurisdictional claim of improper service. Pl.'s Mem. Opp'n Time Warner's Mot. Quash, ECF 22 at 16. This argument is specious. The federal rules permit defendants to simultaneously seek relief and raise a jurisdictional defense without waiver. *See* FED. R. CIV. P. 12(b)(2), (4)-(5) (defendant may move for dismissal based on the court's lack of personal jurisdiction, the insufficiency of process, or the insufficiency of service of process). It simply would be unfair to treat a motion premised on a jurisdictional objection as simultaneously operating as a waiver of that very objection. *United States v. Ligas*, 549 F.3d 497, 503 (7th Cir. 2008) (party's motion to quash does not mean that by making the motion he waived his objection to personal jurisdiction, citing *PaineWebber Inc. v. Chase Manhattan Private Bank (Switz.)*, 260 F.3d 453, 461 (5th Cir. 2001); *Neifeld v. Steinberg*, 438 F.2d 423, 425 n.4 (3d Cir. 1971) (declining to find defendant waived jurisdictional objection

(TIME WARNER CABLE, NOTES FOR LAW ENFORCEMENT AND PSAPS WHEN SERVING SUBPOENAS, COURT ORDERS, AND OTHER LAWFUL PROCESS ON TIME WARNER CABLE SEEKING HIGH-SPEED DATA (INTERNET), TELEPHONE, AND VIDEO SUBSCRIBER DATA (Nov. 16, 2010), *available at* <http://www.timewarnercable.com/corporate/subpoena-compliance.html>). The website referenced by plaintiff provides guidance only for subpoena requests from "law enforcement and PSAPs." PSAP is an acronym for "Public Safety Answering Points," which are emergency call centers responsible for answering calls for police, firefighters, and ambulance services. The website does not apply to the subpoenas issued in civil legal proceedings and is not intended to apply to the plaintiff. Plaintiff's contention that Time Warner waived FED. R. CIV. P. 45(b)'s requirements for proper service for all subpoena requests through directions to law enforcement and emergency personnel on this website is therefore baseless.

when it filed a motion to extinguish a writ of attachment and a motion to dismiss for lack of jurisdiction).

The Court grants Time Warner's motion to quash the subpoena in *Maverick* because the plaintiff did not abide by the requirements of Rule 45(b)(1) and personally serve its subpoena to a named person. The plaintiff is granted leave to re-issue its subpoena to Time Warner within ten days from entry of the order quashing the subpoena. If plaintiff fails to serve its subpoena within 10 days and file proof of service with the Court, the putative defendants listed in the plaintiff's original subpoena to Time Warner, dated September 14, 2010, shall be dismissed.

CONCLUSION

For the reasons set forth above, the Court DENIES Time Warner's Motions to Quash the Subpoena in *Wild*, No. 10-cv-455, and *Donkeyball*, No. 10-cv-1520; and GRANTS Time Warner's Motion to Quash in *Maverick*, No. 10-cv-569. An Order consistent with this Memorandum Opinion will be entered.

SO ORDERED.

March 22, 2011

/s/ Beryl A. Howell
BERYL A. HOWELL
United States District Judge

Exhibit 5

to

Plaintiff's Response to Order to Show Cause - CV 10-04472 BZ

On The Cheap, LLC DBA Tru Filth, LLC v. Does 1-5011, Case No. CV 10-04472 BZ

BOXOFFICE.COM

New MPAA Chief Senator Chris Dodd Delivers Inaugural State of the Industry Speech

Add Comment on **March 29, 2011**

LAS VEGAS -- In his inaugural speech as CEO and Chairman of the Motion Picture Association of America, Inc. (MPAA), Senator Chris Dodd addressed exhibitors and spoke about the strong ties that bind motion picture studios and theater owners and their shared commitment to one of America's greatest industries. The following is the prepared text of Senator Dodd's keynote address at the National Association of Theatre Owners' CinemaCon:

Thank you, John, for that introduction and for NATO's continuing strong partnership. I'd also like to take a moment to thank Bob Pisano, who served as interim CEO this past year and represented the MPAA so well.

Today marks my ninth day on the job as Chairman and CEO of the Motion Picture Association of America. Despite the brevity of my tenure, I wanted to be here today to share with all of you my thoughts on the direction of our industry, and to listen to your concerns at what is both an exciting and challenging time for all of us.

Much of what I will say this morning I know you know, but at a moment like this, it is important that you know what I feel about this industry and the determination I bring to this undertaking.

So let me begin with the obvious: The production and exhibition industries cannot succeed - cannot survive - without each other. If you fail, we fail. And it's just as true that if we fail so will you.

We've come a long way together in the century since the first screening of a feature length motion picture in Jacob Stern's horse barn in Hollywood, California on February 14, 1914. Cecil B. DeMille invited 45 people (all of whom had worked on the film) to view "The Squaw Man," which he made for \$15,000. This premiere, if you want to call it that, was a total disaster.

In order to save some money, Mr. DeMille had purchased second-hand British equipment with ill-fitting sprockets, causing a technical malfunction that allowed the audience to only see the characters' hats, foreheads, boots and feet, and not much else. The economics of our industry have changed, of course, since that day in 1914. And, fortunately, so, too has the technology.

Last year the number of digital and 3D screens more than doubled - and our audience couldn't get enough of it. One in five dollars spent at the box office now comes from 3D. I can't help but wonder what Cecile B. DeMille, Sam Goldwyn, Louis B. Mayer, Jesse Lasky and Adolph Zucker and the rest of these pioneers would say if they could have been among the millions of moviegoers who marvel at the experience of seeing Avatar in a 3D theater. And like moviegoers here at home and all over the world, I can't wait, nor can you, I expect, to see what we come up with next.

But even though so much about our industry has changed over the years, the importance of the theater setting hasn't. Our films are still made to be shown on big screens in dark theaters filled with people. And no matter how our industry continues to evolve, I want all of you gathered here this morning to know that as the new CEO and Chairman of the MPAA, I passionately believe there remains no better way to see a movie than in a theater, and no more important relationship for our studios to maintain than the one we have with you.

So, when we saw box office growth in 2009, we cheered. In 2010 it slowed, and revenues dropped off in the early part of this year. That's not just a concern for you; it's a concern for all of us. But I for one do not believe the sky is falling. Yes, people have a wider variety of entertainment options these days. Yes, gas prices have gone up. But you have seen attendance ebb and flow in the past, and I believe audiences will be coming back to your theaters to see our films because there really is no parallel to the incredible experience that we, together, provide.

You are doing your part by building theaters with great seats, screens and sound systems. This week you'll be seeing some of the exciting projects our studios are working on to fill those seats and screens and sound systems with incredible entertainment later this year.

Thus, on my ninth day on the job, I've come here to commit myself to renewing and strengthening the great American movie-going tradition - and to ask you for your continuing partnership in tackling the challenges we must confront together.

It is, of course, undeniable that we do a fantastic job of providing the American people and others all over the world with quality entertainment. But, in my view, it is just as true that we must do a much better job of educating our audiences and the American people about how we do our job.

Let's begin with perhaps the single biggest threat we face as an industry: movie theft. At the outset, I want you to know that I recognize and appreciate that NATO members are on the front lines every day when it comes to

preventing camcording. Further, I want you to know that the member studios of the MPAA deeply appreciate the efforts you make every day to stop the hemorrhaging of movie theft in your theaters.



I am deeply concerned that too many people see movie theft as a victimless crime. After all, how much economic damage could there be to some rich studio executive or Hollywood star if a movie is stolen or someone watches a film that was stolen? It is critical that we aggressively educate people to understand that movie theft is not just a Hollywood problem. It is an American problem.

Nearly 2.5 million people work in our film industry. The success of the movie and TV business doesn't just benefit the names on theater marquees. It also affects all the names in the closing credits and so many more - middle class folks, working hard behind the scenes to provide for their families, saving for college and retirement. And since movies and TV shows are now being made in all 50 states, Puerto Rico and the District of Columbia, movie theft harms middle class families and small businesses all across the country.

Those who steal movies and TV shows, or who knowingly support those who do, don't see the faces of the camera assistant, seamstresses, electricians, construction workers, drivers, and small business owners and their employees who are among the thousands essential to movie making. They don't see the teenager working their first job taking tickets at the local theater, or the video rental store employees working hard to support their families.

We must continue to work together, pushing for stronger laws to protect intellectual property and more meaningful enforcement of those laws. We must also educate parents and students and everyone else about the real world impact of movie theft on jobs and on local tax revenues, and on our ability to make the kinds of movies and TV shows people wish to see.

At a time when too many Americans are out of work, we remain a major private sector employers, with more than \$140 billion in total wages spread out across a nationwide network of businesses. At a time when our trade deficit continues to spiral out of control, we are, to my knowledge, the only large American industry that maintains a positive balance of trade with every country in the world where we do business.

And speaking of trade, it goes without saying that we are all living and working in a global economy. It is therefore crucial to the survival and growth of the film business that we expand our reach around the world. The economics of our industry depends on the success of our films in all markets, not just our own. This issue is important to every single person in this room. To make the kind of great movies that fill seats in your theaters we must fill theaters in Russia, China, Brazil as well as other markets across the globe.

A larger audience overseas means more resources available for producing films here in America. And that, of course, means more films for distribution and exhibition, more seats filled, more popcorn sold. The good news about our industry is that whenever we're given the chance to compete in the world, we succeed. The bad news is we're not always given that chance to compete.

When China limits the import of non-Chinese films to 20 a year, despite the fact that hundreds of U.S. films are produced each year - including more than 100 by the MPAA member studios - we are excluded from a market that presents huge untapped potential.

I am confident that we can work together to ask Congress and others to protect intellectual property by cracking down on rogue websites that profit from the illegal trafficking of counterfeit movies. After all, you are not just our eyes and ears when it comes to illegal camcording - you are the face of the film industry in your local communities. No one is in a better position to educate the American public about these threats than are you.

After three decades in Congress, I have some idea how to attract the attention of a Congressman or Senator. When you return to your states, invite your local governor, state legislator, congressman and senator to your theater and fill it with those who work with you along with video store employees and their families. Tell them about the importance of these issues to you and to your communities. If you become that educator, you will leave a lasting and indelible impression on those who will make decisions about your future.

That's important not just because we sell a great product, but because all of us - studios, filmmakers and theaters alike - are preserving a great tradition, one that is as central to the American character, as it is important to the American economy.

Which brings me to my last point this morning. What I'm about to say isn't quantifiable in economic terms. I can't put a dollar figure on it for you. I can't give you an unemployment number or some other gripping statistic - but as I stand before you this morning one week into this job, I want you to know that it is as important as all data you will have thrown at you during CinemaCon. Our lives are getting more and more complicated. We are increasingly connected to the world by the power of emerging technologies, but at the same time we seem to be increasingly disconnected from each other by the same technology and stream of information and distractions.

And yet, in the midst of all of this, if you drop by a movie theater in America or anywhere around the world on a Friday or Saturday night you will see neighborhoods coming together. You will see people turning off their phones and BlackBerrys. You will see families and friends settling in for two hours in a darkened theater.

And even though everyone's eyes are on the screen, it is somehow still a communal experience - unlike any other. The value of that shared experience crosses economic, political and even generational boundaries.

Going to the movies together as a community has stitched together the fabric of American society in a way that few other institutions ever have or could, providing a nation of incredible diversity with a common cultural vocabulary and a common understanding of ourselves. What's at stake as we face these challenges is nothing short of the preservation and renewal of this quintessentially American communal tradition. Those who have come before us built the partnership between producers, distributors and exhibitors, which has sustained that tradition for almost a century.

It is my hope, and my commitment to you this morning that when those who follow us look back on this moment in our shared history, they will see that we did not walk away from the challenges we faced. Let them see that we stood together, attacking our challenges with the creativity and courage that have defined the larger-than-life story of American film from its humble beginnings at Stern's stable a century ago.

Like all good stories, this one features occasional moments of high drama. But for me, especially, this is just the first act. And I'm as excited by this new chapter in my life as I was when I first set foot in my local theater on a Saturday morning decades ago.

I'm so pleased that the first performance of this new chapter in my life has been with you. So pleased that the first person to introduce me to an audience, John Fithian, is someone who I've known for half my life and almost all of his.

I'm proud to be a small part of this great American business, and most importantly, I'm honored to be in your company. Your theaters have given America and the world hours of joy and lifetimes of memories. I look forward to working with you closely in the days ahead.

© 2011 BOXOFFICE Media, LLC. All rights reserved.

support@boxoffice.com

Exhibit 6

to

Plaintiff's Response to Order to Show Cause - CV 10-04472 BZ

On The Cheap, LLC DBA Tru Filth, LLC v. Does 1-5011, Case No. CV 10-04472 BZ



Log In | Online Subscription Help | Language Dictionary

Search variety.com **SEARCH**

Home | 4/13/2011 10:11 A.M. | Text size: a⁻ a⁺

Subscribe to VARIETY at 73% off the cover price

Latest News | Latest Reviews | Features | People News | Charts | Opinions | Events | Photos | Videos | VarietyMediaCareers.com

FILM | TV | LEGIT | MUSIC | TECH | INTERNATIONAL | Archives

Technology News

Posted: Wed., Apr. 13, 2011, 4:00am PT

[Share](#) [Print](#)

Joe Biden talks piracy strategy with Variety

VP's involvement with issue extends back two decades

By TED JOHNSON

Exclusive: When Vice President Joseph Biden appeared at a news conference last summer about copyright theft, he compared it to "smashing the window at Tiffany's and reaching in and grabbing what's in" the store.

It was just the kind of hard-line rhetoric that studios and record labels have been yearning to hear from Washington, but even more significant was that it was coming from the nation's No. 2.

One of Biden's friends, former Sen. Christopher Dodd, the new chairman of the Motion Picture Assn. of America, said that Biden isn't just reading from a script when it comes to content protection.

"Joe believes it passionately and understands it intellectually. The marriage of those two doesn't always happen in this town."

If anything, the administration's anti-piracy efforts have been extensive enough to generate criticism from some consumer and digital rights groups that they are too heavy handed. A federal crackdown, which shutdown more than 120 sites trafficking in pirated content, already raised concerns that legitimate sites are being swept up in the effort. And although the issue tends to cross partisan lines, Biden and the administration have strong ties to Hollywood, which was a huge source of donor support for Barack Obama's campaign, and is expected to play a significant role in his reelection campaign.

The White House, however, was mandated to take a greater role in addressing piracy: A law passed in 2008 and signed by President George W. Bush required the establishment of an intellectual property enforcement coordinator, or a so-called "IP czar." Drawing more attention to the issue, Biden has appeared several times with IP coordinator Victoria Espinel, including when she has unveiled a strategic plan in June.

In written responses to a series of questions submitted by Variety, Biden said his involvement with the piracy issue extends back two decades to when he was chairman of the Judiciary Committee, and that his use of the bully pulpit "is really just a continuation of that work."

"Look, piracy is outright theft," Biden said. "People are out there blatantly stealing from Americans -- stealing their ideas and robbing us of America's creative energies. There's no reason why we should treat intellectual property any different than tangible property."



Vice President Joseph Biden told Variety that showbiz needs to do a better job of marketing its anti-piracy pitch.

[Email or Share](#) [Print](#)
[RSS Feed](#) [Bookmark](#)

Get Variety:

[Mobile](#) [Digital](#) [Newsletters](#)

[Subscribe to Variety](#)

-- Advertisement --

We've got great things in "score" for you!

ASSETS / LIABILITIES
WORLD-CLASS MUSICIANS
WORLD-CLASS SCORES
N/A

CALL US: 818.755.7777
FILM MUSICIANS
SECONDARY
MARKETS
FUND
www.fmsmf.org

proud member
HollywoodGreenTeam.org

-- Advertisement --

WHEN MUSIC IS YOUR LIFE

I Create Music
ASCAP EXPO 11
April 28-30, 2011 • Los Angeles, CA

He is quick to say that he considers it more than a problem of just the entertainment industry. "When our military is sold counterfeit equipment that is faulty, it affects our national security. And when cancer patients are sold fake cancer drugs that contain no medicine, it affects public health. These are serious issues for the American people."

"Virtually every American company that manufactures something is getting killed by counterfeiters: clothing, software, jewelry, tires," Biden said. "If an American company has been successful at developing an idea, it's likely getting stolen."

But getting that point across has been difficult.

Although the MPAA and studios have for years run PSA campaigns, they have been of questionable effectiveness.

And while Biden tries to connect the issue to the average worker, in the minds of middle America Hollywood is red carpets, lavish salaries and Charlie Sheen.

"I think the entertainment industry would agree that they have done a poor job in making their case and need to do better," Biden said. "I mean, they have some of the brightest and most creative people working for them."

"They should be able to come up with an intelligent, original and effective public education campaign targeting this issue. To be honest, I am not certain they have dedicated the appropriate resources to this, and I hope they will."

He says that the administration also sees a government role in a public awareness campaign, which is "a big part of our strategy." The Justice Department is providing funds to the National Crime Prevention Council, including messages geared toward kids.

"Kids are taught that it is not right to steal a lollipop from the corner store," he said. "They also need to understand that it is equally wrong to knowingly steal a movie or a song from the Internet."

Biden held an "intellectual property summit" in December, 2009 that brought together cabinet secretaries as well as studio chiefs and reps from other copyright industries, with the intent of mobilizing enforcement efforts. Fox Filmed Entertainment co-chairman and CEO Tom Rothman, who attended another gathering in January that included Attorney General Eric Holder and Secretary of Commerce Gary Locke, said that "in many ways [Biden's] personal commitment to it is a breakthrough for us" as he has tied "the issue's importance to the overall health of the American economy."

Biden doesn't buy the idea that Hollywood's effort to increase enforcement is merely to protect dying businesses.

"The fact is, media companies have already taken significant steps to adapt their business models to keep up with changes in how we watch movies and listen to music," Biden said. "Content is being offered to consumers in a variety of different ways that make it easy and cost-effective for people to access legal material. Anyone who does not understand this should simply talk with one of my grandkids."

In the next few weeks, legislation is expected to be introduced to give federal prosecutors and customs officials a quicker process to get sites offering pirated content shut down, as well as to choke the money supply flowing to foreign sites from payment processors and ad firms.

A version of the bill passed the Senate Judiciary Committee unanimously late last year, but Sen. Ron Wyden (D-Oregon) helped block it from going to the floor because of concerns that it could infringe on free-speech rights. Biden said he's been working with senators to craft legislation "that helps protect property while at the same time respects any potential Constitutional issues. I am hopeful that we will be able to reach an agreement that is agreeable to all parties."

Where Biden says he hopes "we won't need to legislate" is in industry efforts to get Internet providers to inform their customers when they have downloaded or streamed pirated content. Under a "three strikes" law in France, customers who repeatedly view infringing content risk having their service suspended.

Instead, Biden's office has been working with studios and record labels and Internet providers to reach some kind of voluntary agreement to establish standards "that provides greater education to those who might be downloading or streaming illegal content."



**Lindsey Buckingham to be
Interviewed by Sara Bareilles**
Plus over 200 additional panelists!

For the latest news, videos, photos and to register visit
ascap.com/expo

VARIETY CONFERENCES

Britweek Film and TV Summit

April 29, 2011
Beverly Hilton Hotel, Los Angeles, CA

Entertainment & Technology Summit

May 2, 2011
The Ritz-Carlton, Marina Del Rey, CA

2nd Annual International Film Finance Forum

May 13, 2011
Hotel Majestic Barriere, Cannes, France

Film Finance Forum @ Screen Singapore

June 7, 2011
Capella Resort, Sentosa Island, Singapore

3D Entertainment Summit™

June 21-22, 2011
Hilton New York, New York, NY

NY Mobile Entertainment Summit™

June 21-22, 2011
Hilton New York, New York, NY

[View all Conferences and Events](#)



Biden said he sees a shift in China, where piracy is rampant and where Hollywood has long struggled to gain cooperation from the government to address the problem. He said South Korea's strengthened intellectual property laws have led to the "Korean Wave" in entertainment across Asia, and "China's leaders understand this."

When President Hu Jintao visited the U.S. in January, China agreed to take new steps to protect copyrighted material, but Biden said that further efforts will be required "if China is to fulfill its ambition to build a more innovative economy."

Biden is being presented with one of the Recording Academy's Grammys on the Hill awards today.

Contact Ted Johnson at ted.johnson@variety.com

GUEST, HERE ARE OTHER ARTICLES RECOMMENDED FOR YOU...

[Joaquin Phoenix in talks to join Anderson pic](#)

['Pirates of the Caribbean' plans trip to Cannes](#)

[Joe Biden talks piracy strategy with Variety](#)

Powered by 

Read Next Article: [Chromatic chaos reigns >](#)

© Copyright 2011 **RBL**, a division of Reed Elsevier Inc.

[Subscribe](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [About Us](#) | [Advertise](#) | [Contact Us](#) | [Sitemap](#) | [Help](#)

Media: [LA 411](#) | [New York 411](#) | [Variety](#)

Construction: [Reed Construction Data](#)

Business Directory: [HotFrog](#)

Exhibit 8

to

Plaintiff's Response to Order to Show Cause - CV 10-04472 BZ

On The Cheap, LLC DBA Tru Filth, LLC v. Does 1-5011, Case No. CV 10-04472 BZ



Technical report:
An Estimate of Infringing Use of the Internet

January 2011

Version 1.8
Envisional Ltd,
Betjeman House,
104 Hills Road,
Cambridge,
CB2 1LQ

Telephone: +44 1223 372 400
www.envisional.com
piracy.intelligence@envisional.com



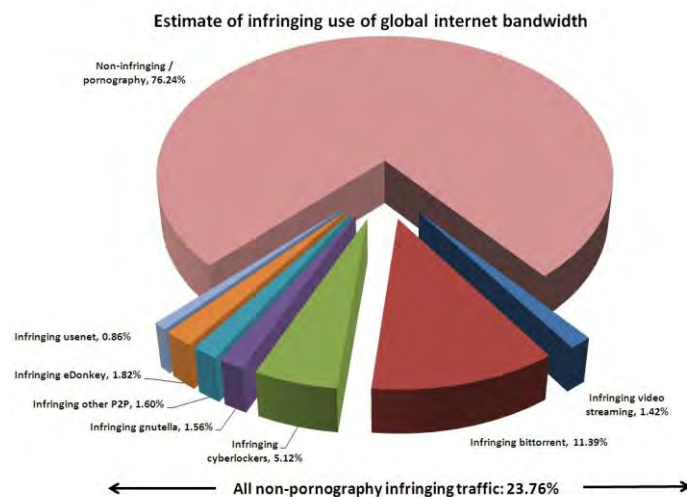
1 Introduction

Envisional was commissioned by NBC Universal to analyse bandwidth usage across the internet with the specific aim of assessing how much of that usage infringed upon copyright. This report provides the results of that analysis and is in three main parts.

- **Part A** examines the internet arenas most often used for online piracy – peer-to-peer networks (with a specific focus on bittorrent), cyberlockers (file hosting sites such as Rapidshare), and other web-based piracy venues (such as streaming video) – and estimates the proportion of infringing content found on each.
- **Part B** is a critical analysis of recent studies from four network equipment and monitoring companies. These companies measured network traffic at multiple (and different) sites worldwide to characterize overall internet usage.
- **Part C** combines the data and analysis from Part A and Part B in an attempt to show what proportion of internet traffic represents unauthorised distribution of copyrighted material.

1.1 Executive Summary

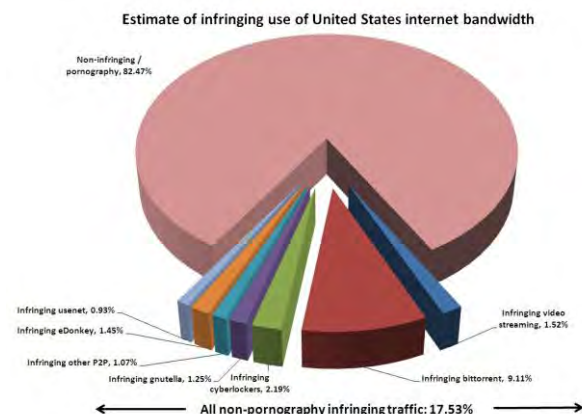
- Across all areas of the global internet, **23.76% of traffic was estimated to be infringing**. This excludes all pornography, the infringing status of which can be difficult to discern.
- The level of infringing traffic varied between internet venues and was highest in those areas of the internet commonly used for the distribution of pirated material.



- **BitTorrent traffic** is estimated to account for 17.9% of all internet traffic. Nearly two-thirds of this traffic is estimated to be non-pornographic copyrighted content shared illegitimately such as films, television episodes, music, and computer games and software (63.7% of all bittorrent traffic or 11.4% of all internet traffic).
- **Cyberlocker traffic** – downloads from sites such as MegaUpload, Rapidshare, or HotFile – is estimated to be 7% of all internet traffic. 73.2% of non-pornographic cyberlocker site traffic is copyrighted content being downloaded illegitimately (5.1% of all internet traffic).

- **Video streaming traffic** is the fastest growing area of the internet and is currently believed to account for more than one quarter of all internet traffic. Analysis estimates that while the vast majority of video streaming is legitimate, 5.3% is copyrighted content and streamed illegitimately¹, 1.4% of all internet traffic.
- Other **peer to peer networks and file sharing arenas** were also estimated to contain a significant proportion of infringing content. An examination of eDonkey, Gnutella, Usenet and other similar venues for content distribution found that on average, 86.4% of content was infringing and non-pornographic, making up 5.8% of all internet traffic.
- In the **United States**, 17.53% of Internet traffic was estimated to be infringing. This excludes all pornography. A breakdown of internet usage yields the following results:

- Peer to peer networks were **20.0% of all internet traffic** with bittorrent responsible for 14.3%. The transfer of infringing content located on these networks comprised 13.8% of all internet traffic.
- **Video streaming made up between 27% and 30% of traffic**, though only a small percentage of this was believed to be infringing (1.52%)
- **Cyberlocker traffic was estimated at 3%** of all network traffic and infringing use was estimated at 2.2% of all internet traffic.



Given the enormous, ever-growing, and constantly-changing size, shape, and consistency of the internet and the use that is made of it means that methodological issues abound when attempting to produce measurements of traffic and content. Yet even given the limitations of the data available, Envisional believes that the estimates produced in this report are more accurate than any that have been published before. This report draws together the data in a way that allows, for the first time, the organisations which can help shape the ways in which users interact and obtain content to understand how much of the internet is devoted to the distribution and consumption of infringing material.

Piracy Intelligence

Envisional Ltd



¹ Mostly from hosts commonly used for pirated content such as MegaVideo and Novamov rather than sites more often used for legitimate user generated content such as YouTube and DailyMotion, for instance.

2 Part A: Internet Usage Assessment

2.1 Introduction

Part A of this report examines the major arenas of the internet known to be used – either primarily or as one of a number of uses – to distribute pirated content. Included in our analysis are:

- BitTorrent
- Cyberlockers
- Video streaming sites
- eDonkey and Gnutella
- Usenet

For each, we estimate the percentage of available content likely to be infringing. Then, in Part C, we translate these individual percentages into estimates of Internet traffic – to do this we rely upon data from studies into network traffic that were conducted by a range of vendors last year and which are discussed in detail in Part B. These individual estimates of infringing traffic are used to yield an estimate of the overall percentage of global internet traffic that results from their use (and which is infringing).

2.2 Executive Summary

Our major findings for each of the four major areas of our investigation follow.

BitTorrent

- BitTorrent is the most used file sharing protocol worldwide with over 8m simultaneous users and 100m regular users worldwide.
- Over 2.72m torrents managed by the largest bittorrent tracker were examined for this report. Our analysis suggests nearly two-thirds of all content shared on bittorrent is copyrighted and shared illegitimately.²
- An in-depth analysis of the most popular 10,000 pieces of content managed by PublicBT found:
 - **63.7% of content managed by PublicBT was non-pornographic content that was copyrighted and shared illegitimately**
 - 35.2% was **film** content – all of which was copyrighted and shared illegitimately

² PublicBT (publicbt.com) is the largest and most popular bittorrent “tracker” worldwide. A recent Envisional survey found that all of the most popular content listed on two popular portals referenced PublicBT trackers. With 2.72 million torrent files available in December 2010, PublicBT is believed to have comprehensive coverage of most files transferred using bittorrent and is therefore a suitable proxy for anyone seeking to assess the percentage of those transfers that infringe copyrights.

- 14.5% was **television** content – all of which was copyrighted and shared illegitimately. Of this, 1.5% of content was Japanese anime and 0.3% was sports content.
 - 6.7% was **PC or console games** - all of which was copyrighted and shared illegitimately
 - 2.9% was **music** content – all of which was copyrighted and shared illegitimately
 - 4.2% was **software** – all of which was copyrighted and shared illegitimately³
 - 0.2% was **book** (text or audio) or **comic** content – all of which was copyrighted and shared illegitimately
 - 35.8% was **pornography**, the largest single category. The copyright status of this was more difficult to discern but the majority is believed to be copyrighted and most likely shared illegitimately⁴
 - 0.48% (just 48 files out of 10,000) could not be identified
- Of all 10,000 files comprising the most popular content held on the PublicBT tracker, **only one was identified as non-copyrighted** (a file containing a list of IP addresses used to help users guard against spam and peer to peer monitoring). There is no evidence to support the idea that the transfer of non-copyrighted content such as Linux distributions makes up a significant amount of bittorrent traffic.⁵
 - Analysis strongly indicates that private bittorrent sites (which would not usually make use of PublicBT) are overwhelmingly used for the purposes of illegitimately sharing copyrighted data.

eDonkey and Gnutella

- Analysis of known copyrighted and non-copyrighted material on the eDonkey network suggests that the vast majority of content held and transferred on the network is likely copyrighted (98.8%).
- Similar analysis using search queries on Gnutella found that most users on the network appeared to be looking for copyrighted content: 94.2% of non-pornographic search queries which could be identified were apparently for copyrighted material.

Cyberlockers

- An examination of 2,000 random links pointing to content held on cyberlockers found that 91.5% of links pointing to non-pornographic material were linking to copyrighted material, or 73.15% of all links.

³ A very small proportion (0.13% of the top 10,000 or 13 individual files) was cracks aimed at removing the copy protection from copyrighted software such as Windows 7 or Microsoft Office.

⁴ For the purposes of this report, the copyright status of any pornography identified is ignored, though the piracy of such content is obviously of interest to the adult video industry (reflected in the many legal suits filed against downloaders during 2010).

⁵ Similar analysis conducted by Envisional in December 2009 found only a single Linux distribution as the only piece of non-copyrighted content in the top 10,000 torrents shared by OpenBitTorrent, then the largest bittorrent tracker online.

Video streaming sites

- A comparison of video streaming site usage estimated that 4.7% of video streaming data traffic is copyrighted content illegitimately streamed from video hosting sites.

Usenet

- Analysis of content posted to a number of Usenet newsgroups found that at least 93.4% of posts contained copyrighted material.

2.3 Discussion: BitTorrent

All available data strongly suggests that bittorrent is the most used file sharing protocol worldwide. Part B of this report contains data conservatively estimating that bittorrent usage makes up 14.6% of *all* internet bandwidth worldwide. Envisional consistently measure over eight million users simultaneously connected to the bittorrent network and the distributor of two of the most-used bittorrent clients, uTorrent and BitTorrent Mainline, claims that the clients have over 100 million unique users worldwide and 20 million daily users⁶.

This section of the report aims to establish what proportion of the data transferred through bittorrent is legitimate and approved by the content owner and what proportion is illegitimate and copyrighted. This is a complicated task. The estimate provided here is produced from a number of data points but primarily from a major investigation into the activities of the largest public bittorrent tracker, PublicBT.

2.3.1 Tracker Analysis

Much of the communication on bittorrent takes place with the aid of a central server called a *tracker*. A tracker helps users on bittorrent find those who are already downloading or uploading the file or files in which they are interested. The tracker records the IP addresses of those actively involved in obtaining or distributing a particular file and then shares them with other bittorrent users when requested.⁷

Trackers also record data on each **torrent or file** which they track: this data includes the 'hash' of that file (a unique code that identifies that file alone) as well as the number of **seeds** (users holding an entire copy of the file), **leechers** (users in the act of downloading), and (in most cases) total completed **downloads**. Trackers do not tend to record file names.

The largest tracker worldwide is the **PublicBT tracker**. At the point that this analysis was conducted, it held information on over 2.7m individual torrents⁸. Launched in 2009, the tracker



became the most-used tracker for bittorrent swarms during 2010. PublicBT is simple to use, open to any bittorrent user, and free. It has also proved very reliable during its life to date. PublicBT does not cover *every* file available on bittorrent: bittorrent users are free to create torrents using any trackers of their choice and some niche content – such as sport broadcasts or technical ebooks – may be more often found at private trackers which require

⁶ <http://www.businesswire.com/news/home/20110103005337/en/BitTorrent-Grows-100-Million-Active-Monthly-Users>

⁷ Trackers are not the only way to obtain IP addresses: bittorrent clients can also communicate through a decentralised network overlay. Additionally, some clients will swap IP addresses of known downloaders or uploaders of a specific file in a transaction known as 'peer exchange', though they must have already managed to locate the other client in the first place. However, trackers are used as the first port of call in almost all torrent downloads and are likely to be the source of a significant proportion of the IP addresses gathered by a client.

⁸ <http://publicbt.com/>

registration. However, analysis of the most popular 100 torrents on two popular portals (ThePirateBay, the most used portal worldwide and Torrentz⁹) found that every single torrent listed could be found on the PublicBT tracker, indicating that PublicBT can be assumed to have close to comprehensive coverage of the content that is most downloaded on bittorrent. The sheer size of the tracker also means that such coverage will be deep and broad.

Envisional was able to gather data on **every file tracked by PublicBT** on a specific day. This data was then used in an attempt to estimate the amount of legitimate against illegitimate and copyrighted content carried by the tracker. On the day of analysis (a weekday in mid-December 2010), PublicBT held information on **2.72m individual torrent swarms** and managed connections from just over **19.5m peers**.¹⁰

The analysis below examines the characteristics of all the 2.72m torrent swarms found on PublicBT. A detailed study was also made of the 10,000 torrents managed by PublicBT that had the most active downloaders, in order to better understand the make-up of the most sought-after content on bittorrent. An analysis of these swarms found that pornography, film, and television were the most popular content types. Further, with pornography excluded, **only one identified swarm in the top 10,000 offered legitimate content** (a file holding a list of IP addresses used to guard users against spam and peer to peer monitoring).

2.3.2 Summary analysis

On the day chosen for analysis of PublicBT, **2,721,440 torrents** were being managed by the tracker. These are unique files but the figure does not mean 2.72m different films or television episodes or pieces of music. There may be many different copies of a specific film title available through PublicBT – for instance, at different file sizes or in different formats or different qualities (as an example, seventy-one different versions of the film *Inception*, one of the most popular titles at the time of analysis, were located in the top 10,000 torrents).

Each file available on bittorrent is identified by a unique ‘hash’ – a unique code that identifies that file and no other.¹¹ PublicBT thus held information on the active downloaders and uploaders of just over 2.7m unique hashes.

⁹ www.thepiratebay.org and www.torrentz.me

¹⁰ This does not mean 19.5m individual users: a peer connected to two torrents will be counted twice in that total of peers due to the nature of bittorrent. It is not possible to know the average number of swarms to which an average user is connected at any one time. However, even assuming that each user is connected to nineteen torrents tracked by PublicBT (a very high estimate judging on anecdotal evidence) would still mean that 1m individual users were connected to PublicBT, around one-eighth of the total simultaneously connected bittorrent population of 8m. A more likely possibility is that most users connect to far fewer swarms and that PublicBT activity reflects a large proportion of public bittorrent transfers.

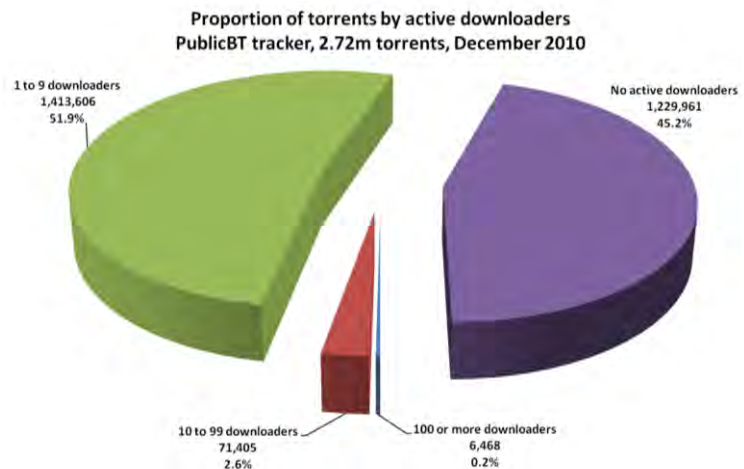
¹¹ A “hash” is a unique alpha-numeric sequence used to identify files (movies, music, documents, etc) on bittorrent. On the bittorrent network, the hash is generated by the SHA1 algorithm which creates a small identifier from a large file (such as a movie). Even trivial modifications to the original file results in a completely different hash.

Content analysis

On the day of analysis, most upload and download activity was concentrated amongst a **small number** of those 2.7m torrents with 34.9% of all peers involved in the top 10,000 (just 0.37% of all torrents). There was an **enormous long-tail of content** which had only a few or no seeds or a few or no leechers.

The chart shows the breakdown of all 2.72m swarms according to the number of downloaders (commonly called leechers) attached to each swarm¹². Clearly, most of the swarms had only a small number of active downloaders or no active downloaders at all.

- 0.2% of torrents (6,468) had 100 or more downloaders
- 2.6% of torrents (71,405) had from ten to 99 downloaders
- 51.9% of torrents (1,413,606) had from one to nine downloaders
- 45.2% of torrents (1,229,961) had no active downloads



A similar spread was evident for seeders (users holding a complete copy of the file). For almost **half of all torrents** (1.32m or 48.5%), no seed was connected.

On the other hand, a very small overall proportion of content attracted large numbers of downloaders, representing a large proportion of all connected users. As stated above, torrent swarms with 100 or more downloaders represented just 0.24% of the available 2.72m torrents, but more than one in three – 30.4% - of all peers connected to PublicBT. Torrents with ten or more downloaders represented 2.6% of the 2.72m available torrents but over half – 53.9% - of all peers.

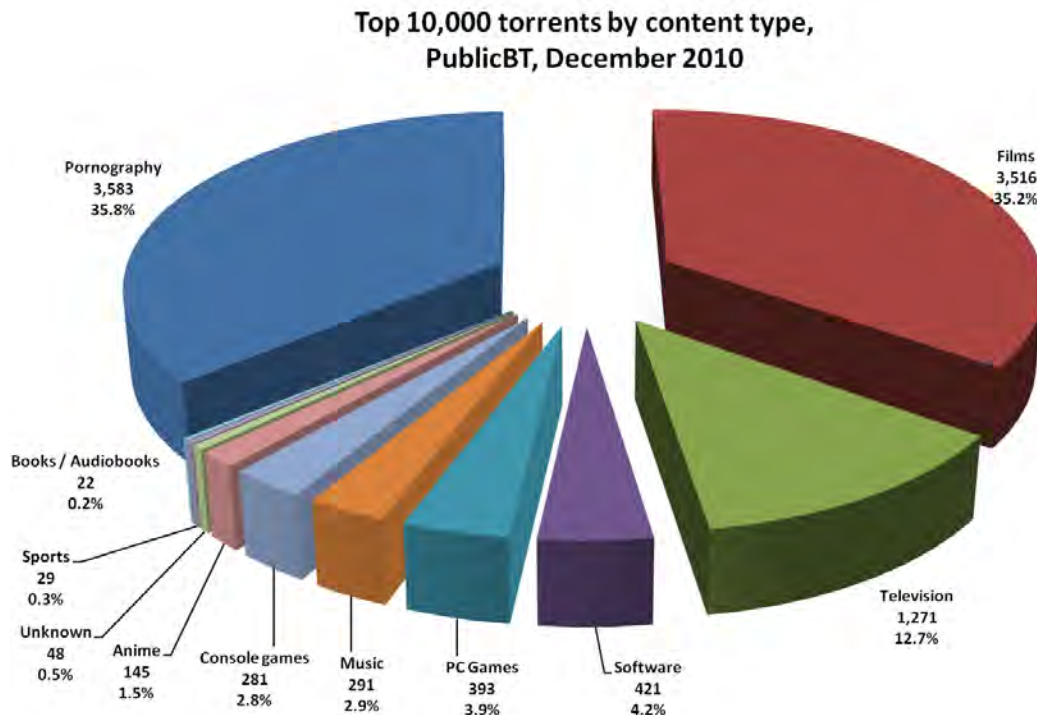
¹² This report uses the term 'swarm' even where no participants were actively sharing content (for instance, where there were no downloaders or no seeds). Technically perhaps, a torrent for which there is a tracker and a seed but no downloader should be known as a 'potential swarm' or similar but the term 'swarm' is retained for the sake of simplicity and understanding.

Analysis of the top 10,000 torrent swarms

To determine the percentage of infringing content associated with PublicBT, Envisional made a thorough analysis of **the top 10,000 swarms** (as determined by the number of downloaders). This is a small sample of the overall number of torrents (0.37%) but represents **34.9% of all peers** connected to PublicBT. To put it another way, more than one-third of all connections to PublicBT were interested in just 0.37% of the swarms managed by the tracker, showing a strong interest in a very small proportion of content. The seeds connected to these most popular 10,000 swarms were 35.5% of all seeds while the downloaders were 33.8% of all leechers.

The content being shared by each swarm in the top 10,000 was verified in almost every case using various methods¹³. Overall, **9,952 of the top 10,000 swarms were identified and confirmed** (99.52%) with only 48 swarms containing unknown content.¹⁴

The chart shows the distribution of swarms by content type with video dominating overall. Pornography video was the largest single type at 35.8% of all of the top 10,000 torrents. Film was the second largest type at 35.2%, followed by television episodes at 12.7%. Japanese anime episodes added a further 1.5% and sports broadcasts another 0.3%. These results mean that **85.5% of all of the top 10,000 torrents were video content of some kind**.

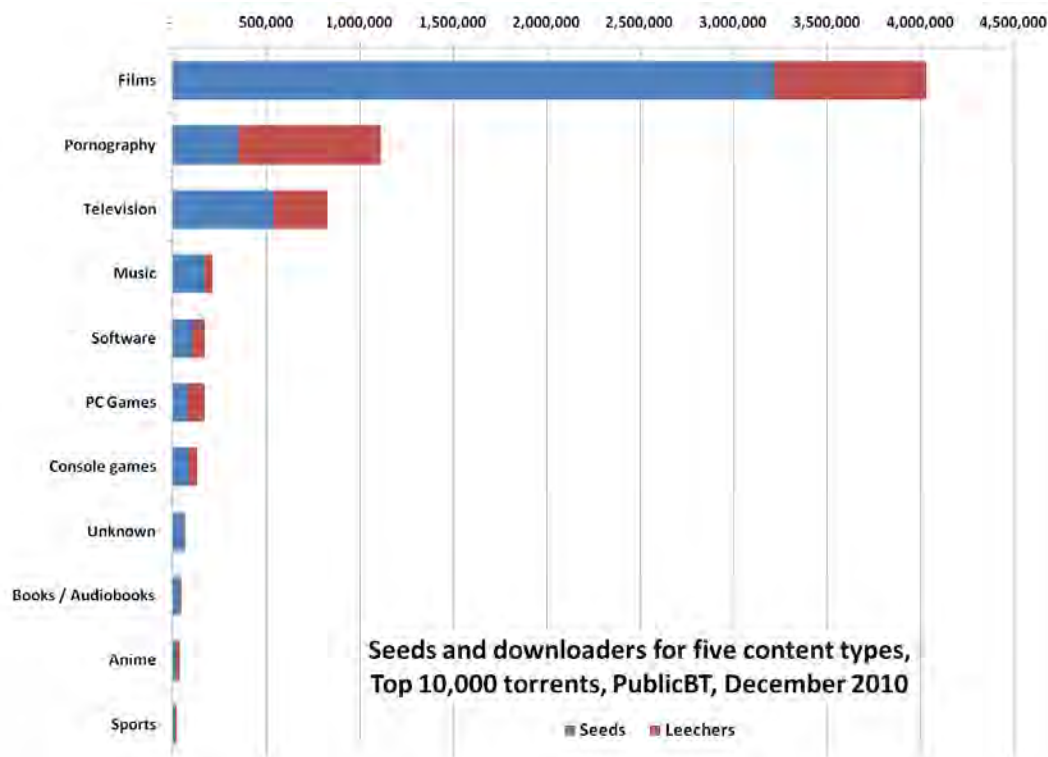


¹³ In most cases, the hashes for each torrent were checked against a range of torrent portals for verification. For many video files, a section of the file was downloaded and viewed.

¹⁴ Note that the analysis of the top 10,000 swarms contained here does not include 139 files which contained enough leechers to merit inclusion within the top 10,000 but were found to be fake. Fake files are often uploaded to bittorrent by interdiction companies hoping to confuse downloaders or by virus and malware distributors. The top 10,000 is therefore **the top 10,000 non-fake files** – or to put it another way, the top 10,139 files with the fake files removed.

Software comprised 4.2% of all of the top 10,000 torrents with computer games adding 6.7% (PC games were the largest proportion at 3.9% and console games contributed 2.8%). Music was 2.9% of the total with books (including comics) and audiobooks adding 0.2%. The remaining 0.5% of torrents could not be identified.¹⁵

The chart below looks at the number of seeds and downloaders for each content type within the top 10,000 torrents: again, video content – particularly film – gathered the largest number of seeds and downloaders (indicating strong demand and strong supply)¹⁶. In total, just over **4.0m peers were seeding or downloading a piece of film content** located in the top 10,000 torrent swarms on PublicBT at the point that this sample was taken. This is 59.2% of all peers connected to the top 10,000 swarms.



While pornography was the largest single type by numbers of torrents, there were many fewer total peers, principally because there were many fewer seeds than for film content. 828,000 peers were seeding or downloading television content and there were much lower numbers for the remaining content types in the top 10,000 torrents. Across all categories, peers connected to swarms for video content (films, television, anime, sports, and pornography) made up 88.4% of all peers in the swarms for the top 10,000 torrents.

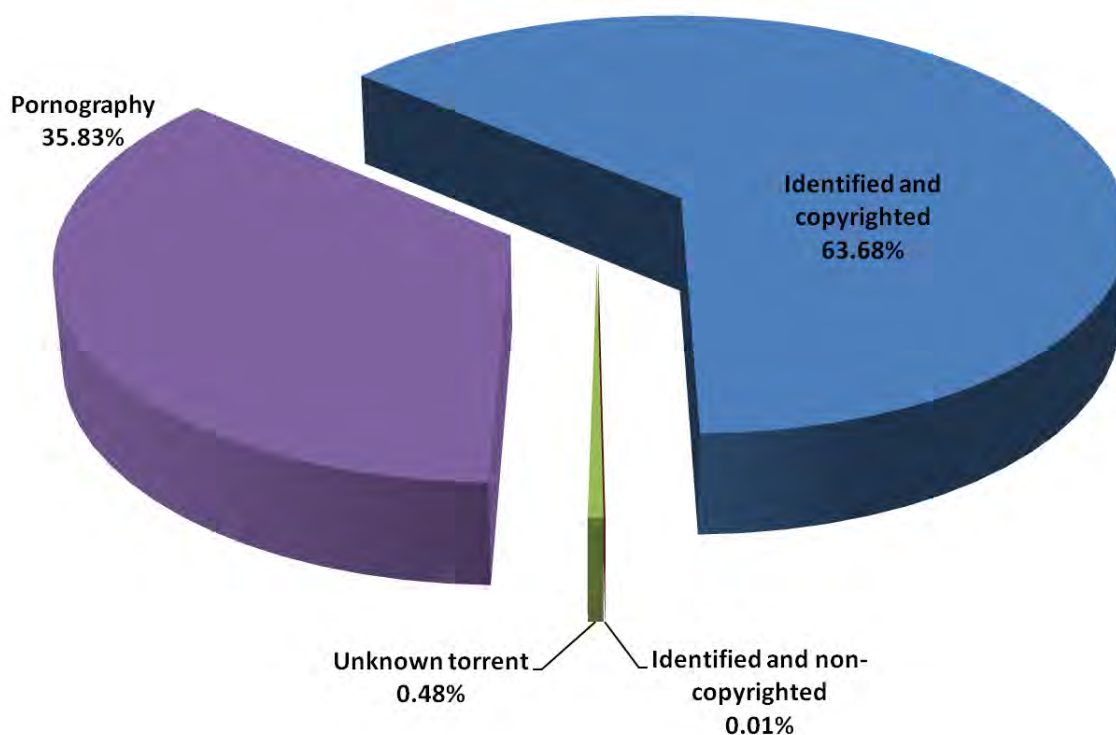
¹⁵ Overall, this analysis is similar to that conducted by Envisional in December 2009 on the OpenBitTorrent tracker, though the current effort successfully identified significantly more torrents. The earlier analysis could not identify 25.0% of the top 10,000 torrents though most of these unidentified torrents were believed to be pornography. The more recent analysis reported here suggests that this belief was correct.

¹⁶ Numbers for seeders and downloaders were taken from PublicBT during the period of analysis.

Proportion of copyrighted material

As noted, the contents of 9,952 swarms were identified and verified. Excluding the swarms containing pornography (3,583 swarms or 35.83%) provides 6,369 pieces of verified content. Of these identified swarms, **only one was found to contain non-copyrighted content**. This was a torrent containing a list of IP addresses used to help peer to peer users block spam results and fake content.¹⁷

**Copyrighted material in top 10,000 torrents
tracked by PublicBT, December 2010**



With the pornography content discarded, this means that at a minimum, **99.24% of the top 10,000 files managed by the PublicBT tracker** were copyrighted material with the rest of the content unknown (0.75%) or non-copyrighted (0.01%).

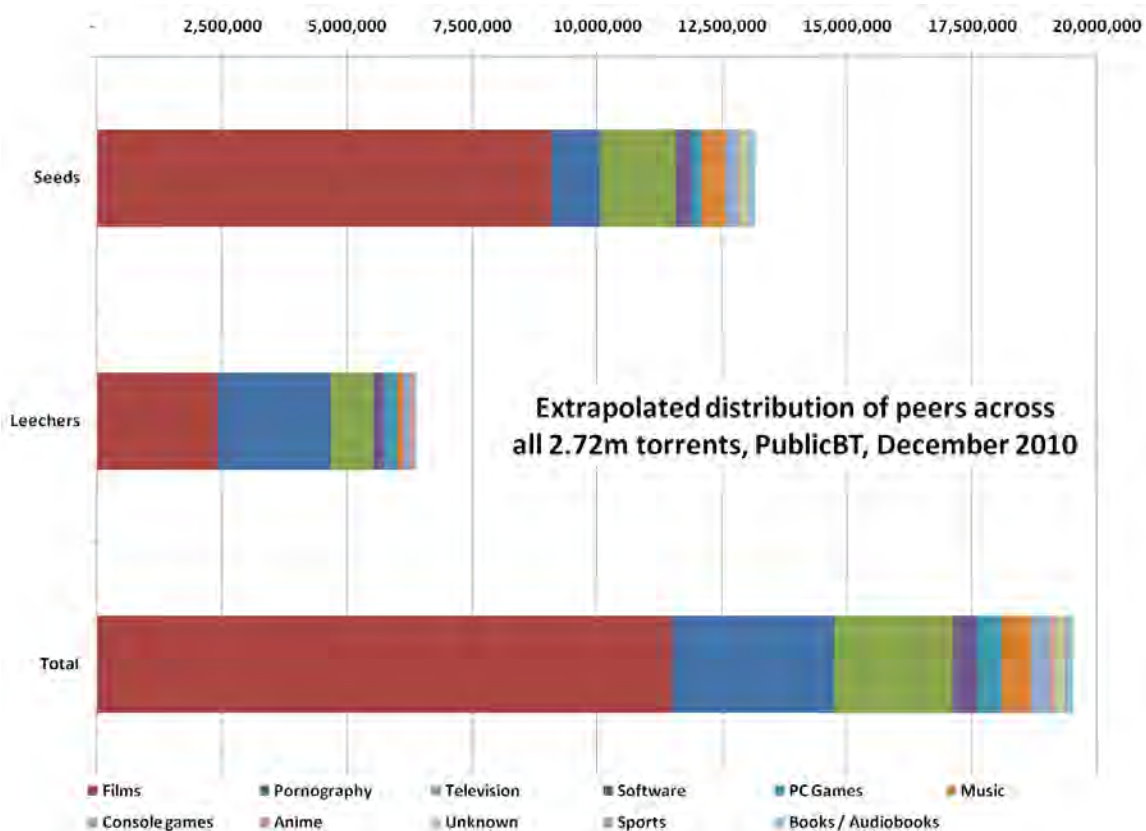
Analysis of content from outside the top 10,000 torrents found a similar dominance of copyrighted material. Five samples, each of 100 torrents, were taken from various points in the long tail of PublicBT content. Discarding

¹⁷ The file was named "hostiles.txt". The torrent hash was a55603e3b98fb51fd05fb2ed3fbc2b2c6d254c6e. The results mirror the Illinois State University study conducted by Jon Peha and Alex Mateus (Carnegie Mellon University) in which it is noted: "...there is no evidence to support the hypothesis that the transfer of Linux distributions is a driver for the use of P2P, even among users that do not use P2P for copyrighted material." See *Dimensions of P2P and digital piracy in a university campus*: http://www.ece.cmu.edu/~peha/dimensions_of_piracy.pdf

pornography, no non-copyrighted content was located in these samples though there was a slightly higher spread of unknown material (as might be expected from less popular content).¹⁸

Extending the results

If the figures underlying the chart above for the top 10,000 torrents are extrapolated to all of the content present on PublicBT, it would mean that on the day of analysis, **11.5m peers were seeding or downloading film content** through the PublicBT tracker, **2.4m peers were seeding or downloading television content**, 3.2m pornography, 593,000 seeding or downloading music, and 862,000 games.¹⁹ The chart shows the result of this calculation and the table over provides further details.



¹⁸ This result accords with past analysis which have indicated that the majority of content offered on torrent portals is infringing. For instance, Judge Steven Wilson noted in his Isohunt decision that "In a study of the Isohunt website, [Dr. Richard] Waterman [of the University of Pennsylvania] found that approximately 90% of files available and 94% of dot-torrent files downloaded from the site are copyrighted or highly likely copyrighted."

http://www.wired.com/images_blogs/threatlevel/2009/12/fungruling.pdf

¹⁹ For instance, 69.05% of all seeds for the top 10,000 swarms were involved in swarms for film content (3,220,293 seeds). Assuming that 69.05% of seeds across all swarms were involved in swarms for film content provides an extrapolated figure of 9,084,608 seeds.

	Seeds			Downloaders (leechers)			Total
Content type	Seeds in top 10,000 swarms	Percent of all seeds in top 10,000	Estimated seeds across all swarms	Downloaders in top 10,000 swarms	Percent of all downloaders in top 10,000	Estimated downloaders across all swarms	Total peers (seeds plus downloaders)
Films	3,220,293	69.05%	9,084,608	812,648	37.73%	2,404,271	11,488,879
Pornography	347,618	7.45%	980,648	766,157	35.57%	2,266,725	3,247,372
Television	538,607	11.55%	1,519,437	289,426	13.44%	856,285	2,375,723
Music	170,989	3.67%	482,369	37,399	1.74%	110,647	593,016
Software	99,645	2.14%	281,104	71,259	3.31%	210,824	491,928
PC Games	78,543	1.68%	221,574	91,059	4.23%	269,404	490,978
Console games	85,118	1.83%	240,122	44,148	2.05%	130,615	370,737
Unknown	58,687	1.26%	165,559	6,630	0.31%	19,615	185,174
Books (incl. audiobooks)	41,621	0.89%	117,415	2,777	0.13%	8,216	125,631
Anime	12,536	0.27%	35,365	24,211	1.12%	71,630	106,994
Sports	10,337	0.22%	29,161	8,046	0.37%	23,805	52,966

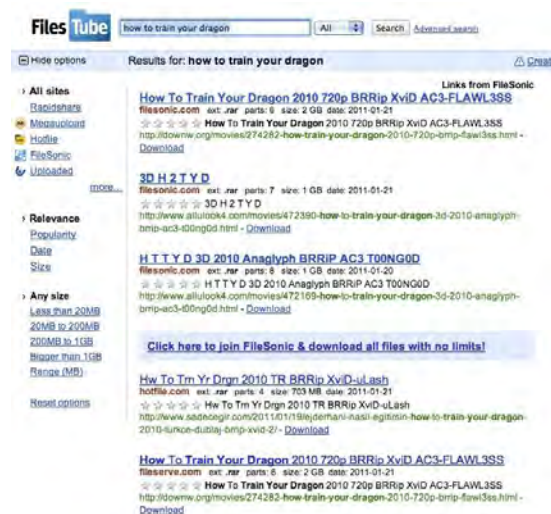
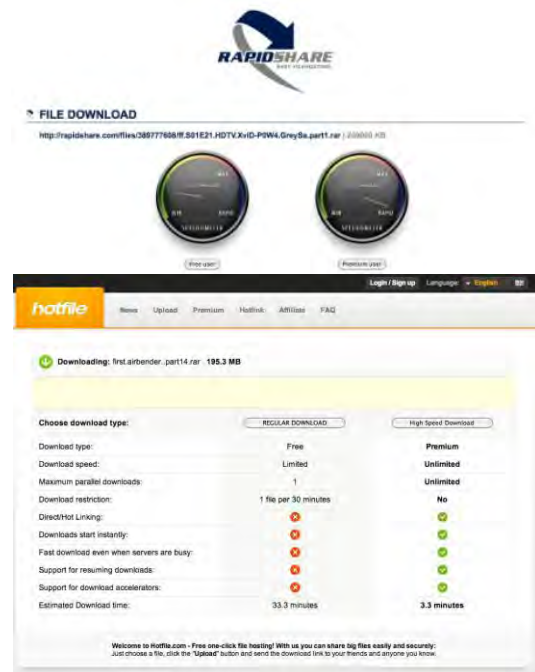
2.4 Discussion: Cyberlockers / File hosting sites

Over the last two years, various technological factors such as the decline in the cost of data storage combined with the increasing use of the web as the most important and central part of the internet for most users have led to the appearance and increasing use of what have become widely known as 'cyberlockers': centralised file storage services to which individuals can upload material for access by themselves or others. There are a number of widely used cyberlockers such as **MegaUpload**, **4Shared**, **Rapidshare**, and **Hotfile**. Envisional monitor over one hundred different cyberlockers.

To store or access content on a cyberlocker, users need only a web browser – unlike P2P programs like bittorrent and eDonkey which require a dedicated client application. Also, direct downloading from a cyberlocker can be quicker than P2P on high bandwidth connections, more anonymous than P2P, and is often (at least at present) less prone to malware, viruses, and spoofing.

Users can freely upload any material to such sites and are then provided with a link with which anyone can then access that content. For non-paying users, content remains on the service for a limited period, can only be downloaded a certain number of times, and can only be downloaded after a waiting period of a minute or so while the potential downloader is presented with various advertisements. Premium memberships (typically costing around USD \$13 / €10 a month) allow content to be stored for longer and – more importantly for downloaders – grant those prepared to pay with instant and high speed downloads of any content (not just their own) stored on the service.

Significantly, the vast majority of cyberlockers do not allow the content they hold to be searched in the same manner as a torrent portal: there is no way to query Rapidshare or MegaUpload for every file they hold that matches the phrase 'Lost' or 'Spiderman', for instance. This would seem to limit the attraction of these sites for piracy purposes but, as with many pieces of web-based technology, they were quickly co-opted for the purposes of containing and distributing pirated material. Hundreds of third-party **cyberlocker indexing sites** (such as FilesTube, right) and **link sites** (such as Warez-BB, shown in the screenshot below) have appeared in the last



couple of years which collate and make available links to pirated content held on cyberlockers. A user of such a site uploads a file to Rapidshare or another cyberlocker and then posts the link to that file on one of the many bulletin boards, forums, or indexing sites that cater to cyberlocker users. Any user can then click to obtain the material. As noted above, downloads are free, though users must sit through a wait time before the download can start and speeds are limited *unless* a premium account is purchased – this brings downloads that begin instantly at speeds which are usually as fast as the user's broadband capacity.

Topics		
<ul style="list-style-type: none"> ➤ [RS.com] An Education (2009) DVDRip XviD-ALLIANCE Description: 200MB links Single Extraction No Pass [Goto page: 1 ... 7, 8, 9] ➤ [RS/HF] Centurion (2010) DvDrip AC3 [Eng] - LoIR [Goto page: 1, 2] ➤ [HF] MKV Movie Collection (300-400 MB) - Powered By ~SHUFOL~ Description: No password / Ready Back ups / Single Extraction / IMDb / plot [Goto page: 1 ... 7, 8, 9] ➤ [RS.com] The Football Factory LIMITED DVDRip XviD-SCREAM Description: User Rating: 6.7/10 (5,982 votes) For all the Scoopers fans!! [Goto page: 1, 2, 3] ➤ [RS.com] Menace II Society (1993) BRRip Xvid HD 720p + Eng S ➤ [MULTI] The Losers (2010) - DVDR-ALLIANCE ➤ [MS][RS][MU] Killers R5 LINE XVID - MCB 700 MB 1LnkMS Description: Action Comedy Thriller 700MB Interchangeable 1 LnK MS ➤ [RS/HF/RS/NL] The Last Airbender (2010) Encoded XviD CAM Description: One Link + 400MB + 200MB NFO Single Extraction ➤ [RS.com] Carandiru (2003) DVDRip *AC3* Description: COOLGuE Release ➤ [RS.com] Toy Story 1+2 Dvdrip.Xvid ➤ [RS] Airplane! / Flying High! Description: My First Movie Upload [Goto page: 1, 2, 3] ➤ [MULTI] Nanny McPhee And the Big Bang (2010) ➤ [MULTI] Killers R5 LINE XVID - IMAGINE Description: (Ashton Kutcher, Katherine Heigl) - (Action) Full Posters - Screen - S.E. - No Pass [Goto page: 1, 2, 3] 	<ul style="list-style-type: none"> 133 28 126 32 5 1 8 9 14 0 31 5 30 	<ul style="list-style-type: none"> baszczudesu 3782 Papicholo 857 ~SHUFOL~ 1069 bravekoh 1592 CoolStuff 225 shirfan 55 movee08 300 kennyjam17 523 emmyyus 825 Bluesmiley 2 Goon_1337 1040 sudeshna.putu 173 @shenif 1357

Screenshot from WareZ-BB link site

The practice is not as large as bittorrent (and the need to pay for a premium account before the full benefits can be realised is one of the reasons why), though it has grown significantly over the last two years. The largest cyberlockers are among the most popular web sites in the world: for instance, ComScore estimates that



4Shared and MegaUpload have around 78m unique users each month (more than twice as many as ThePirateBay, the largest bittorrent portal); RapidShare 60m unique users; and Hotfile 53m unique users. Alexa ranks 4Shared.com as the 66th most popular site in the world and MegaUpload as the 67th most popular. The usage studies in Part B estimate traffic to web-based cyberlockers and centralised file hosts at around 7% of all internet usage, though this varies significantly from country to country and may be as low as 2.5% for North America and the United States. Sandvine estimates overall usage of Rapidshare and MegaUpload together as 5.1% of all internet traffic.

Methodology

Envisional's Discovery Engine technology (an automated search, identification, and classification system for internet content) was employed to crawl the internet to locate links to content stored on ten large cyberlockers like Rapidshare and MegaUpload. The intention was to locate as many links as possible and then to analyse those

links to see what type of content had been uploaded to the cyberlocker (e.g., a film, television episode, ebook, photograph) and to determine whether that content was likely copyrighted or not.²⁰ A random sample²¹ of 2,000 links gathered by the Discovery Engine was taken and analysed and the content type noted²². The results are below together with the proportion of each found to be copyrighted.

Content type	Links found		Copyrighted	
	#	%	#	%
Films	715	35.8%	709	99.2%
Television	169	8.5%	162	95.9%
Pornography	401	20.1%	345	86.0%
Music	201	10.1%	189	94.0%
Games	187	9.4%	155	82.9%
Software	199	10.0%	180	90.5%
Books / Audio books	52	2.6%	38	73.1%
Other / unknown	76	3.8%	30	39.5%
Total	2,000	100.0%	1,808	90.4%
Excluding pornography	1,599	79.95%	1,463	91.5%

As with bittorrent, much of the analysed content – over 90% – appeared to be copyrighted. The vast majority of films, television episodes, music, software, and games were copyrighted and available on cyberlockers illegitimately.

²⁰ An obvious shortcoming of this approach is the difficulty of finding links to non-copyrighted files legitimately stored on cyberlockers as such use does not generally involve publicizing a link onto the wider internet (personal photos, for instance, would likely be shared with family and friends via an email link). Still, it is reasonable to assume that while cyberlockers such as Rapidshare may host a non-trivial amount of non-copyrighted content, the *popularity* of that content – and hence the number of downloads and amount of bandwidth utilised – is likely limited.

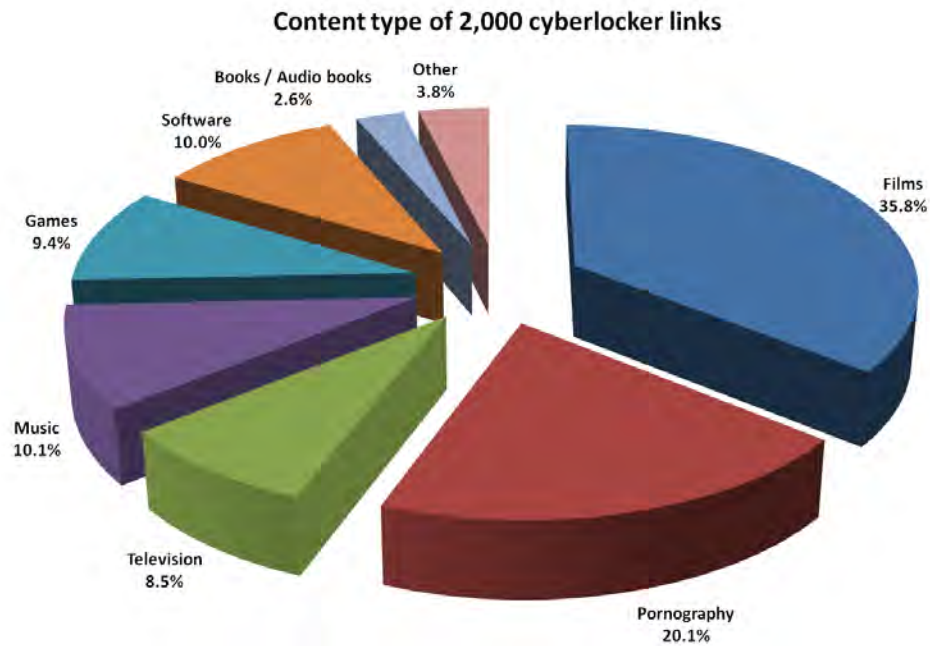
For example, Rapidshare announced a bandwidth upgrade to 600 Gbps (75 GBps) in March 2010 (<http://en.wikipedia.org/wiki/RapidShare>). This enabled a theoretical maximum of 194.4 PetaBytes/month to be transferred. Applying an 80% utilization factor results in an estimate of 155 PetaBytes of content transferred each month. With 50 million unique monthly users of Rapidshare (a figure taken from Google Trends), this amount of content equates to each user of the service downloading 4.15 movies per month. If films were replaced by collections of non-copyrighted photographs, those 50m unique users would need to download 307 collections of photos each month (assuming that each batch of photos comprised forty photos at 250Kb each = 10MB) were Rapidshare's bandwidth to be used entirely by this type of content.

The focus in this example is on downloading for, as Sandvine noted in its 2009 report: "Rapidshare is used primarily for data acquisition (*there is relatively little upstream traffic*) [emphasis added] and is generally not popular with average broadband subscribers." See: <http://bit.ly/sandvine>

The basic fact is that experienced internet analysts and researchers can find very little evidence that the bandwidth consumed by cyberlockers is used in the distribution of non-copyrighted content to any substantial extent.

²¹ The sample was selected using a random number generator.

²² Many cyberlockers only allow files of a particular size to be uploaded. This means that files greater than this size must be uploaded in parts. The common way to do this is to break the larger file into smaller 'Rar' files generated by the Rar archiving tool. The files will typically be named 'Filename.rar' and 'Filename.ra1' or 'Filename.part01.rar' and 'Filename.part02.rar'. When the Rar files are unarchived, the resulting file is re-created. For the purposes of this analysis, a file with multiple parts was treated as being a single file.



There is a larger proportion of smaller files such as eBooks and music on cyberlockers than on bittorrent. This accords with Envisional's experience of how each file sharing method is used. For example, with a cyberlocker, uploading is a simple one-click process that lasts only for the time necessary to upload the full file. There is no long-term uploading relationship and the upload occurs once at the decision of the uploader. Bittorrent, on the other hand, relies on a group of individuals exchanging small parts of a large file and the initial file creation process and upload process takes time and some knowledge. Seeding files is an ongoing process which can require long-term usage of a bittorrent client and an internet connection. Finally, files are uploaded only when and if another individual decides to download the file on offer – an element of uncertainty not present with cyberlockers. All in all, these differences provide cyberlockers with an ease-of-use advantage over P2P and users may respond by uploading a greater number of smaller files such as music and books.

2.5 Discussion: Video streaming

Every recent report which examines the recent past and immediate future of internet usage (see Part B) identifies streaming video as the fastest growing segment of bandwidth consumption worldwide. Led by YouTube, determined by most research to consume at least 5% of all internet bandwidth alone, the use of streamed video has become widespread across the entire internet. Sandvine believe that 'real-time entertainment' (streamed content consumed as it downloads) comprises 26.6% of all internet usage; Cisco state that 'streaming' traffic is 27.8%;

and Arbor Networks estimate that 25% of traffic is streamed video or audio of some kind. All studies also cite the significant rise in this segment of internet usage and all predict further growth in this area.

Unlike bittorrent, eDonkey, and cyberlocker usage, experience indicates that most usage of video streaming is benign and poses no threat to copyright: Facebook videos of parties, news reports, YouTube rants, and so on. The rise in video streaming has gone hand-in-hand with the increase in user generated content pushed onto the internet and it is obvious to anyone with a passing familiarity with sites like YouTube that the majority of content currently uploaded onto such sites is produced by users and is not copyrighted or is uploaded legitimately by content owners (for instance, of the top ten 'most viewed' videos on YouTube, six are legitimately-uploaded music videos totalling 850m views).

However, there can also be no question that there is a significant amount of pirated content available which has been uploaded to video hosting sites across the world. There is an obvious appeal to internet users of films and television episodes which begin seconds after a user clicks play rather than requiring a wait for the download to complete before consumption. Browser-based and easy-to-use, video streaming web sites are a major concern of content owners and it is not difficult to find pirated versions of any major film or television series with a few minutes of persistence.

YouTube itself prevents most users from uploading content longer than fifteen minutes in length and has added tools such as digital fingerprinting to ensure that copyrighted material is identified and banned but the site has been host to a broad section of unauthorised copyrighted material in the past. Other video hosts are often much

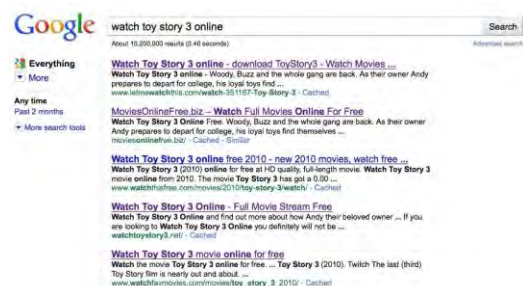


less willing to implement proactive barriers to pirated content, allowing longer-duration uploads while enabling high quality streaming and refusing to implement filtering for copyrighted material.

In a similar fashion to the way that cyberlocker link sites have co-opted cyberlockers for piracy purposes, so video link sites have done the same for video hosts. Sites such as **LetMeWatchThis** and **Movie2k** index pirated content held on video hosts to present users with numerous choices for the latest film or television show. For instance, LetMeWatchThis currently offers forty-three separate working links to view *Inception* on different video hosting sites. Video link sites either embed Flash-based video players which stream content hosted on sites like MegaVideo or directly link viewers to the hosts that contain the streaming video.



Streaming videos of pirated content can also be found using a normal search engine. For example, querying Google for terms such as 'watch toy story 3 online' reveals a plethora of linking sites and blogs in the top ten results which offer links to streams of unauthorised pirated versions of the film.



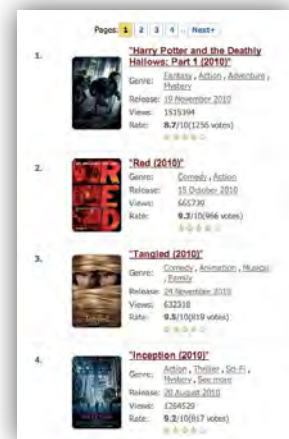
The most popular piracy video link sites gather millions of visitors each month. ComScore estimate LetMeWatchThis to have 6.5m unique users each month and Movie2K to have 5.0m unique users, for example.

Estimating pirated usage of video streaming

Estimating the amount of total video streaming bandwidth that may be unauthorised copyrighted material is difficult. Unlike bittorrent, where the PublicBT tracker manages millions of separate swarms, there is no major repository of video which can be taken to provide a good overall indicator of total video use: YouTube is certainly dominant in this space but as mentioned, there are a number of factors which ensure that YouTube is currently minimally used for new pirated content. The widespread nature of video use across the web means that a link analysis as performed for cyberlockers would be unlikely to gather accurate data.

After reviewing a number of possible methodologies, the best approach to this difficult area was deemed to be one which compared the popularity of index sites used to locate streaming pirated content with index sites used to locate pirated material available via bittorrent.

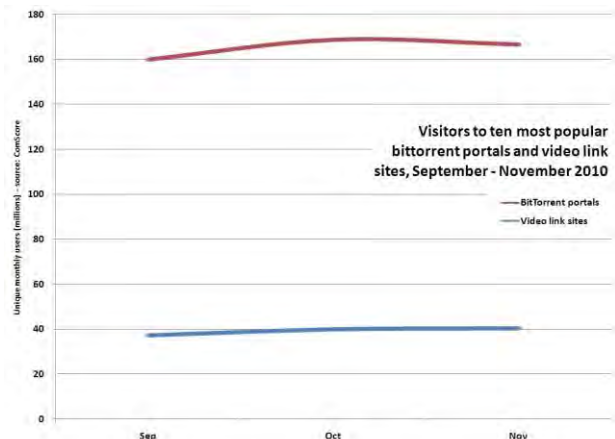
Web metric providers such as ComScore and Alexa offer statistics on the number of daily or monthly visitors to bittorrent portals such as ThePirateBay, IsoHunt, and Torrentz, the main sites from which the vast majority of bittorrent users find links to the pirated content that they ultimately download using the bittorrent protocol – and which then results in the large amount of bittorrent traffic seen in the usage studies. In the same way, users of video streaming sites use portals such as LetMeWatchThis, ZMovie (right) and Movie2K to locate links to pirated content they wish to see, clicking through to the video hosts where the content is hosted. By comparing the known audience for bittorrent portals with the known audience for video link sites, a rough estimate of pirated usage may be possible.



ZMovie

Both types of sites – bittorrent portals and video streaming link sites – are almost entirely devoted to pirated content: scans of the content available on bittorrent sites like ThePirateBay and IsoHunt and video link sites such as LetMeWatchThis and TVShack find close to no content which is not copyrighted (and that this content is unpopular when and if it does exist). It can then be broadly assumed that visitors to video streaming link sites will be consuming pirated material.

The chart shows data from ComScore for monthly unique users to the top ten bittorrent portals and the top ten video link sites worldwide from September to November 2010. Clearly, bittorrent is a much more popular activity on this measure: on average across these three months, the top ten video link sites had an audience just under one-quarter (23.71%) that of the top bittorrent portals – or to put it another way, the



bittorrent portals had slightly over four times as many visitors (4.22x).

Assuming that the end result of a visit to a bittorrent portal is the same as a visit to a video streaming link portal – that a user locates and downloads or streams the content in which they are interested – then the total data which is then transferred must be considered. The amount of data required to consume a file via a video streaming site is usually significantly less than when downloading a film or television episode from bittorrent. The file size is usually much smaller (and hence the final quality of what the user views is often poorer – which may be one reason why bittorrent is more popular as it provides higher quality content).

For example, each link for the ten most recent films posted to a popular video linking site was analysed and the streaming file to which it pointed on a video host was measured in terms of file size. On average, the streamed content comprised 384.2MB. Data taken from the analysis of PublicBT earlier in this report found that the average file size for downloaded films was 937.7MB. On this estimate, it means that each film downloaded via bittorrent results in almost 2.5 times (2.44x) as much data for the same content as via video streaming (or, stated another way, consuming a film via video streaming results in less than half the network traffic (40.97%) as downloading it via bittorrent).

$$\frac{\text{Visitors to Video Link Sites}}{\text{Visitors to Bittorrent Portals}} \times \frac{\text{Streaming File Size}}{\text{Bittorrent File Size}} = \text{Ratio of streaming traffic to bittorrent traffic}$$

As such, video link site traffic may generate the amount of data equivalent to **9.71% of all bittorrent traffic** (video link site visitors as a proportion of bittorrent portal visitors divided by the difference in average file size consumed). The detailed calculation is shown below which, assuming that Sandvine's estimate of bittorrent traffic is correct (14.56%), finds that the traffic which comes from video link sites that link to pirated material is equivalent to **1.42% of all internet traffic**.

A. Amount of all internet traffic measured as bittorrent (Sandvine) ²³	14.56%
B. Amount of all internet traffic measured as video streaming of any kind (average estimate from Sandvine, Arbor, and Cisco – see Part B of this report)	26.5%
C. Video link site visitors as a percentage of bittorrent portal visitors	23.71%
D. Average streamed file size from video link sites (384.2MB) as a percentage of average film file size downloaded via bittorrent (937.7MB)	40.97%
E. Estimated pirated data usage of video link sites as a percentage of all bittorrent internet traffic (C * D)	9.71%
F. Estimated pirated data usage of video link sites as a percentage of <i>all</i> internet traffic (A * E)	1.42%
G. Estimated pirated data as a percentage of all streaming traffic (F / B)	5.34%

Given the difficulty of gathering data in this area, these figures should be taken as a cautious estimate.

²³ Sandvine estimates bittorrent traffic to be 14.56% of total internet usage and is the only company to provide a figure specifically for bittorrent based on a large amount of data – Ipoque did estimate bittorrent usage but its estimate is based on a small amount of total data from a low number of monitoring sites. Other companies talk of “peer-to-peer” usage and not “bittorrent usage”.

Also, Sandvine measured peer-to-peer usage as a lower proportion of all internet usage than some other providers (particularly Cisco) leaving open the possibility that bittorrent usage may be higher. As Sandvine are the only company to provide data for bittorrent alone, their estimate will be used but should likely be taken as a minimum.

2.6 Discussion: Other file sharing arenas

Analysis was also made of three other file-sharing arenas where copyrighted content is generally distributed: eDonkey, Gnutella, and Usenet.

2.6.1 eDonkey

The eDonkey peer to peer network is one of the oldest peer-to-peer networks still in existence. It is heavily used in mainland Europe (particularly in Spain, Italy, and France). Envisional measure between 2.5m to 3m users simultaneously connected to the network or a decentralised network overlay for the network called Kad. Sandvine estimates eDonkey traffic at 1.5% of all internet usage globally.

The most accurate way to calculate the proportion of pirated material available on eDonkey would be through analysis of one or more eDonkey servers and the content which is indexed and downloaded. However, such servers are high priority targets for anti piracy organisations and would be unlikely to cooperate with a request for oversight of the content which they have indexed. While it is possible for anyone to establish a server, doing so helps facilitate the distribution of content between users connected to that server and with much content felt to be pirated, this was not deemed to be a suitable way to research this area.

Instead, searches were made using the eMule client and Envisional's own peer-to-peer monitoring technology for one hundred pieces of content for which results would likely be pirated (new films and television episodes, for instance) and one hundred pieces of content for which results would not be pirated (content legitimately allowed to be distributed such as live concerts from some artists and books licensed under Creative Commons).²⁴ In each case, the most popular instances of each content type were chosen. The number of complete sources for each piece of named content were counted.

The amount of legitimate content available amounted to **1.2%** of all the content located on the network. This is a tiny proportion and while the research is not methodologically perfect, it does indicate that the majority of material held and transferred on eDonkey (in this analysis, **98.8%**)²⁵ is likely copyrighted.

²⁴ For example, copyrighted film content such as *The Dark Knight* and *Avatar* and television episodes from series such as *Lost*, *Heroes*, and *Doctor Who* and non-copyrighted material such as live concerts from Pearl Jam, books licensed under Creative Commons such as Cory Doctorow's *Makers*, and films like *Steal This Film*.

²⁵ Though this figure excludes pornographic content for which searches were not made.

2.6.2 Gnutella

The Gnutella network is widely used for the distribution of music as well as other content. Envisional's own Gnutella crawler estimates the network to have around 2.0m users at any one time since the closure of the company behind the LimeWire client at the end of 2010. Sandvine estimates Gnutella usage at 1.9% globally and the network is particularly popular in North America.

Envisional analysed the searches made by users on the network²⁶. A sample of 3,500 search queries were examined for the content type to which they most likely referred and as to whether the content sought was copyrighted or not²⁷. The table below shows the results. The 'copyrighted' column only includes those queries for which the copyright status could be clarified.

Content type	Search queries		Copyrighted	
	#	%	#	%
Film	144	4.12%	144	100.00%
Television	254	7.26%	254	100.00%
Pornography	453	12.95%	Unknown	Unknown
Games	59	1.69%	53	89.90%
Music	1,920	54.87%	1,786	93.00%
Other	108	3.11%	105	96.70%
Unknown	560	16.00%	Unknown	Unknown
Total	3,500	100.0%	2,342	66.9%
Excluding pornography and unknown	2,487	71.06%	2,342	94.2%

It was not possible to determine the copyright status of the pornography for which users searched. A large section of 'unknown' queries included many queries in Japanese (around one-fifth of all unknown queries) which could not be accurately translated. However, a majority of such Japanese queries for which translation was possible indicated that the search was likely for a pornographic video of some kind.

While it seems clear that music content is the most popular on the network – a finding supported by other research into Gnutella – there are some obvious methodological issues with using this process to calculate copyrighted content. For instance, search queries do not necessarily translate into downloads, particularly if the query cannot be matched exactly. Nonetheless, it is telling that 94% of the non-pornographic searches that could be identified were for copyrighted material. A similar study by Professor Richard Waterman of the University of

²⁶ Clients which act as 'supernodes' receive search queries from other peers on the network and other supernodes.

²⁷ For instance, a search for 'Lady Gaga telephone' was assumed to be a search for the audio version of this song. A search for 'Lady Gaga telephone video' or 'gaga video' was assumed to be looking for a music video. A search for 'telephone' could not be classified as any particular content type and was thus categorised as 'unknown'.

Pennsylvania which used a sample of 1,800 files found that 98.8% of files requested on Gnutella were either copyrighted or highly likely to be copyrighted.²⁸

2.6.3 Usenet

Usenet is one of the oldest communications arena on the internet – and as with many areas of the internet, the system was quickly co-opted by those wishing to spread pirated content after its initial appearance. A few years ago, a small web site (recently shut down after legal action in the UK²⁹) created the ‘NZB’ system for quickly retrieving large files from Usenet. NZB files opened up Usenet to a much larger potential audience and offered third-party services an opportunity to create businesses centred around facilitating access to Usenet. Some of these businesses, such as Usenext in Germany, are now multi-million Euro operations (Usenext had revenue of €30m in 2007). Significantly, almost all committed Usenet users pay for access: Usenext charge between €10 and €25 Euros per month and similar services do the same. The necessity to pay for access to Usenet has certainly limited the spread of the system as a way to obtain pirated content but Envisional believes that up to half a million users connect regularly to Usenet to obtain pirated content³⁰. The usage studies cited in Part B that look explicitly at Usenet estimate overall traffic devoted to the arena at between 0.5 – 1% of overall internet usage.

Usenet began as a text-based medium meant for sending simple text messages. This remains the only real use for the system outside of transmitting files and it is unlikely that this aspect of the service takes up more than a tiny percentage of overall Usenet usage. In order to determine usage of Usenet for the transmission of copyrighted material, a random selection of 100 newsgroups from the many thousands available through the Giganews Usenet provider³¹ were sampled and the last 100 complete files or messages posted to each newsgroup analysed. The copyright status of each post was checked. Text messages made up 3.2% of all posts; **93.4% of all posts** (all of which were files) contained copyrighted content; 2.3% were likely copyrighted; and for 1.1% of posts (all files), the copyrighted status could not be identified.

Thus at least 93.4% of sampled posts made to Usenet contain copyrighted content. However, given the size of these files (for instance, a typical film posted to Usenet will be at least 700MB in size), each post containing copyrighted content will dwarf the size of any text posts made. In terms of the actual amount of data transferred over the network, copyrighted material likely makes up more than the 93.4% of individual posts.

²⁸ See <http://www.scribd.com/doc/31284309/Arista-et-al-v-Lime-Wire-et-al-summary-judgment>.

²⁹ <http://newzbin.com/>

³⁰ An estimate made by reference to the amount of traffic received by major Usenet providers and NZB sites as well as through analysis of the published accounts of a large Usenet access provider in Europe.

³¹ <http://giganews.com/>

3 Part B: Internet Usage Assessment

3.1 Introduction

This part of this research report critically evaluates recent research produced by a number of companies that offer different pictures of overall internet usage. Four main studies of bandwidth usage were examined. Each study was released during the second half of 2009 and were conducted by four network monitoring companies, mostly using data gathered during 2009:

- Sandvine Incorporated
- Arbor Networks
- Cisco
- iPoque

Each of the studies had the same broad aim: to illustrate the protocols and applications which are used across the internet and to show how much of the internet's bandwidth is used by each. For instance, each study analysed the amount of internet traffic taken up by peer to peer technologies or by streaming video as well as more traditional pursuits such as normal web browsing and email. However, direct comparison between each was problematic.

Each study:

- used different monitoring techniques
- was based on varying periods of time, examined different amounts of data and looked at different areas of the world
- used different categorisations for types of traffic

The categorisation issue is one of the largest problems with comparing the four studies. For instance, all four studies identify streamed video as a growing portion of internet traffic. However, each study uses a slightly different method of identifying this traffic and sometimes include the content in a different broad category which also comprises other items. For instance, Arbor Networks uses the simple term 'Video' to mean progressive video downloads; Sandvine speaks of 'Real-time entertainment' to denote video and other content such as audio which is consumed as it is downloaded or streamed; Cisco classifies 'Internet video to PC' as video or television on demand viewed on a computer; while iPoque uses the category 'Streaming' to refer to any kind of streamed audio and video. Some categories appear to be fairly consistent across all four studies: for example, all use 'P2P' as a broad identifier for known peer to peer networks. However, it was not always possible to determine the range of peer to peer networks detected by each monitoring company (though the largest known networks such as bittorrent, eDonkey, and Gnutella seemed to be always included), nor to know their rate of successful detection.

None of the four studies can be accepted without reservation, though some offered more confidence than others. The following sections discuss each of the four studies in detail, outlining the main points, the basis of the findings, and the methodological issues which are attached to each of them.

3.2 Sandvine: 2009 Global Broadband Phenomena

Monitoring period: September 1st – 22nd 2009

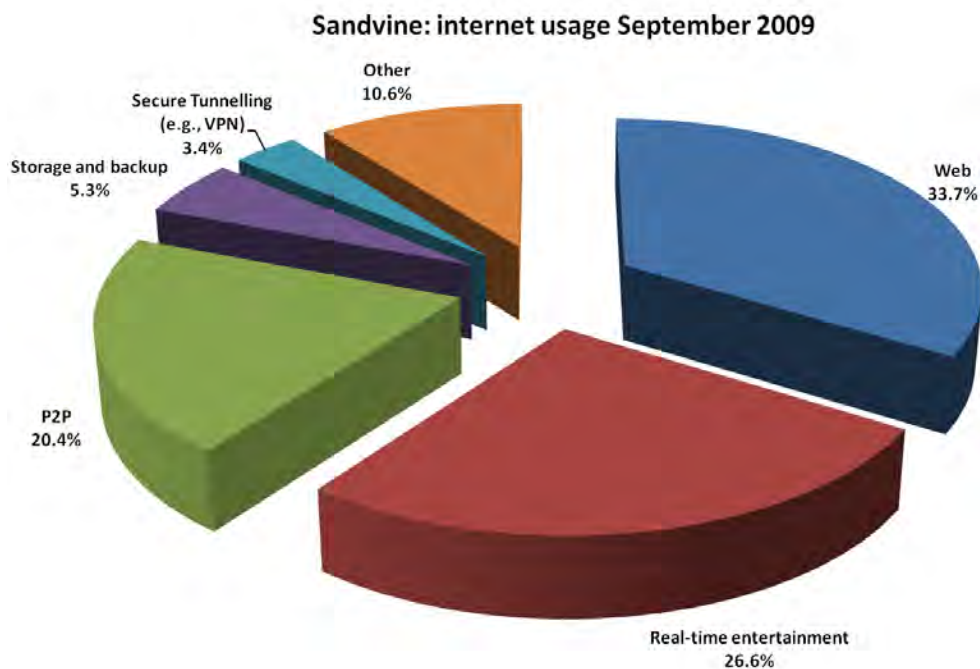
Monitoring locations: 22 ISPs in five regions: nine from North America, five from Europe, four in the Middle East and Africa, two in the Caribbean and Latin America, and two in Asia-Pacific

Number of subscribers: 24 million.

Amount of traffic monitored: Unknown

P2P traffic: 20.4%

Streaming video traffic: 26.6% (categorised as 'real-time entertainment' – content consumed as it is downloaded)



Other points:

- 'Storage and backup' services (which include cyberlockers and web-based backup services) consume 5.3% of internet traffic
- P2P proportion is 18.5% in North America
- Streaming video proportion is 26.7% in North America
- 'Real-time entertainment' category (streamed or buffered video or audio) more than doubled from 12.6% in 2008 to 26.6% in 2009.
- Significant variation between regions

3.2.1 Methodology

Sandvine is a Canadian-based network monitoring provider. The company's 2009 *Global Broadband Phenomena* report repeated analysis completed in 2008. The study contained a detailed categorisation of content and thorough analysis of current trends based on 24 million subscribers from twenty ISPs in five regions, including nine ISPs located in the United States. Their data is based on internet traffic flowing through Sandvine's monitoring equipment and captures application usage from the subscriber's perspective. The company is also able to detect visitors to some popular web sites (such as YouTube and Rapidshare). Analysis looks at the average subscriber in a number of regions across the world and also uses a weighted global average of data to provide overall figures.

The main finding of the Sandvine study is the identification of a *"dramatic shift' from bulk download 'experience later' behaviour towards real-time 'experience now' application"*. Sandvine uses a category termed 'Real time entertainment' to denote streamed video or audio which is consumed as it is downloaded. In 2009, this category accounted for 26.6% of total traffic, an increase from 12.6% in 2008. The increasing consumption of video content by internet users is a common theme within most of the studies.

Sandvine issued a 2010 *Global Broadband Phenomena* update as this Envisional report was being finalised. The 2010 report³² did not provide data for worldwide traffic but found that 'real-time entertainment' continued to grow, accounting for up to 43% of peak time traffic in North America (with Netflix measured at 20% of peak time downstream traffic alone). Peer to peer traffic remained very important: bittorrent was found to comprise nearly 17% of downstream traffic during peak periods in North America and 37% in Latin America.³³

3.2.2 Discussion

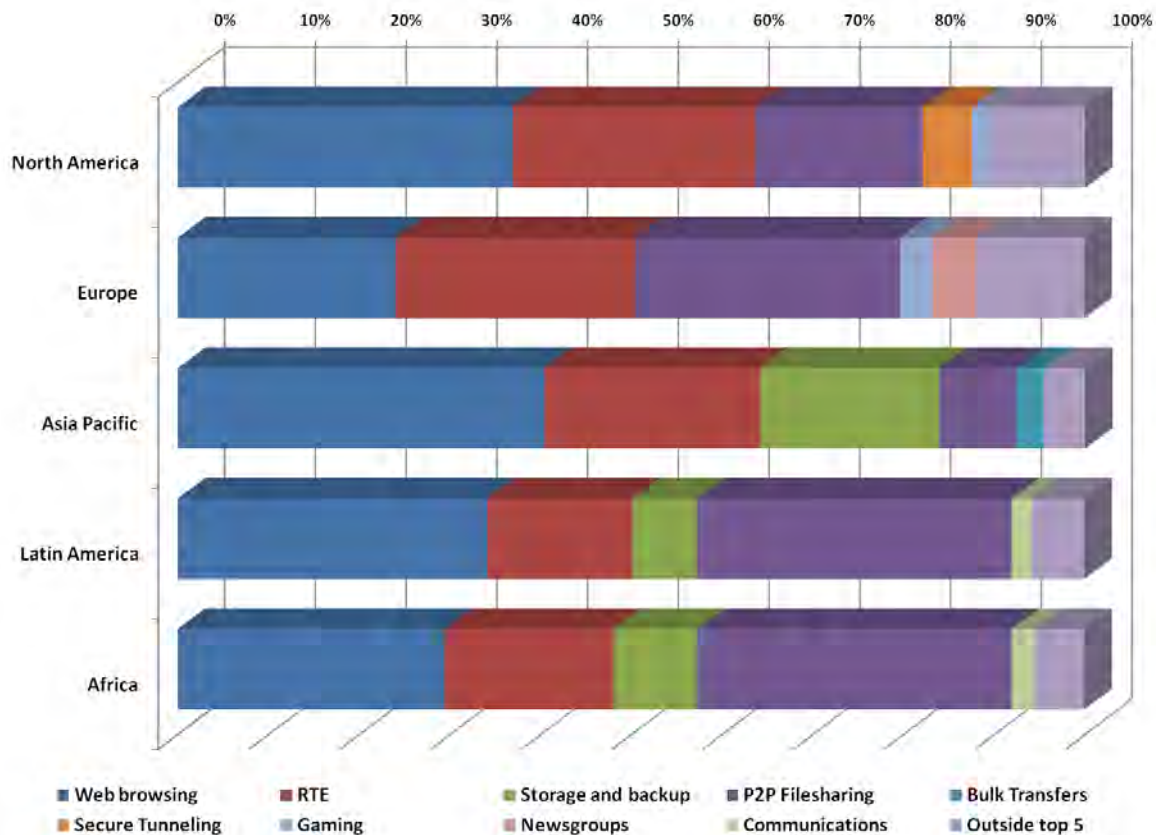
The chart on the page above illustrates the top five categories in terms of traffic detected worldwide by Sandvine. Web surfing contributes just over one-third (33.7%) of all traffic with the 'Real-time entertainment' (RTE) category responsible for more than one-quarter (26.6%, more than doubling in size since 2008). While much of this activity takes place through the web or browser it is separately categorised by Sandvine. Peer to peer filesharing then adds a further one-fifth (20.4%) of all traffic. More than 80% of internet traffic is thus taken up by these three categories alone. A 'storage and backup' category refers to cyberlocker sites such as Rapidshare which allow centralised file hosting and retrieval via the web (and which are often used for piracy purposes).

³² http://www.sandvine.com/news/global_broadband_trends.asp

³³ There are some areas in which the 2010 report raises questions - for instance, in highlighting Zshare as the most popular cyberlocker in Europe. All other information gathered by Envisional from our own and other data sources cite Rapidshare, Hotfile, and MegaUpload as the three most-used cyberlockers with Zshare a second- or even third-tier site. For instance, data from ComScore place Zshare as the eighth most popular cyberlocker with one-tenth of the number of visitors of the most popular site.

Sandvine's report also makes clear that internet usage varies greatly across the world, a theme that is repeated in the reports from Cisco and iPoque. The chart below shows the top five categories of traffic in the different monitoring regions used by Sandvine. Some of the main differences are as follow:

- Web browsing as a portion of internet traffic ranges from 24% in Europe to 40% in Latin America
- P2P usage ranges from 8.6% in the Asia Pacific region to 34.7% in Africa
- Storage and backup services (online file hosts) are under 1.9% of internet usage in North America but 19.7% in Asia Pacific (influenced by the heavy use of centralised 'web-hard' services like PDBox in Korea, a location where Sandvine have monitoring equipment installed)
- Gaming traffic is (just) one of the five largest categories in North America and Europe but nowhere else.
- Newsgroups provide 4.7% of traffic in Europe but do not appear in the top five in any other region.
- Real-time communications traffic appears in the top five categories for Latin America and Africa but not elsewhere.

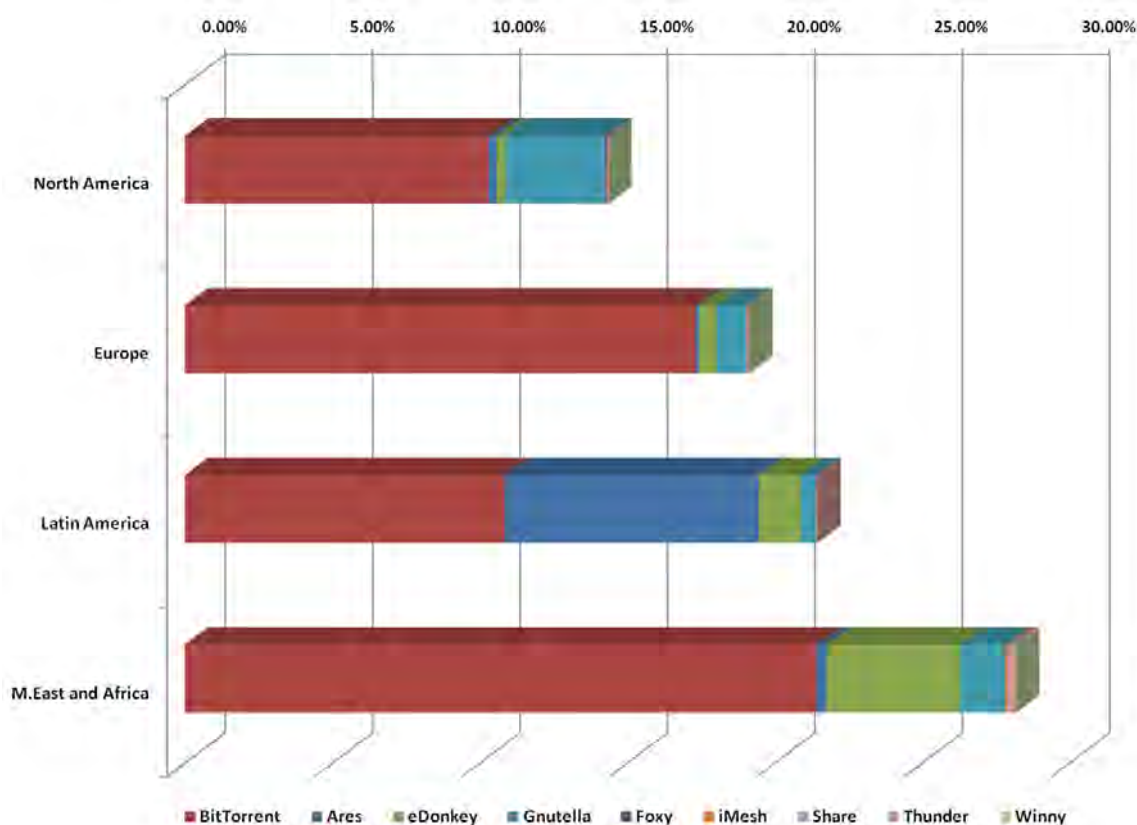


3.2.3 Additional detail

Sandvine provided Envisional with further detailed information on traffic from individual P2P applications as well as a small number of central web sites³⁴. This additional data was broken down by four regions.

Sandvine tracked nine P2P applications: BitTorrent, eDonkey, Ares, Gnutella, iMesh (a client that connects to a legitimate music network), and four clients predominantly used in Asia: Foxy (a variant of Gnutella), Share and Winny (two popular Japanese networks), and Thunder (a download manager / P2P application popular in China where it is usually known as 'Xunlei'). Absent are some well-known protocols such as Shareaza and DirectConnect. It is unknown whether Kad, the decentralised sister network to eDonkey, was classified under the eDonkey header. (Peer to peer television (P2P TV) clients such as PPLive and PPStream are classified as 'Real time entertainment'.)

The chart below shows the percentage use of these P2P networks in each of the regions examined by Sandvine. Again, usage differed from region to region. The data is the average downstream usage of each application.

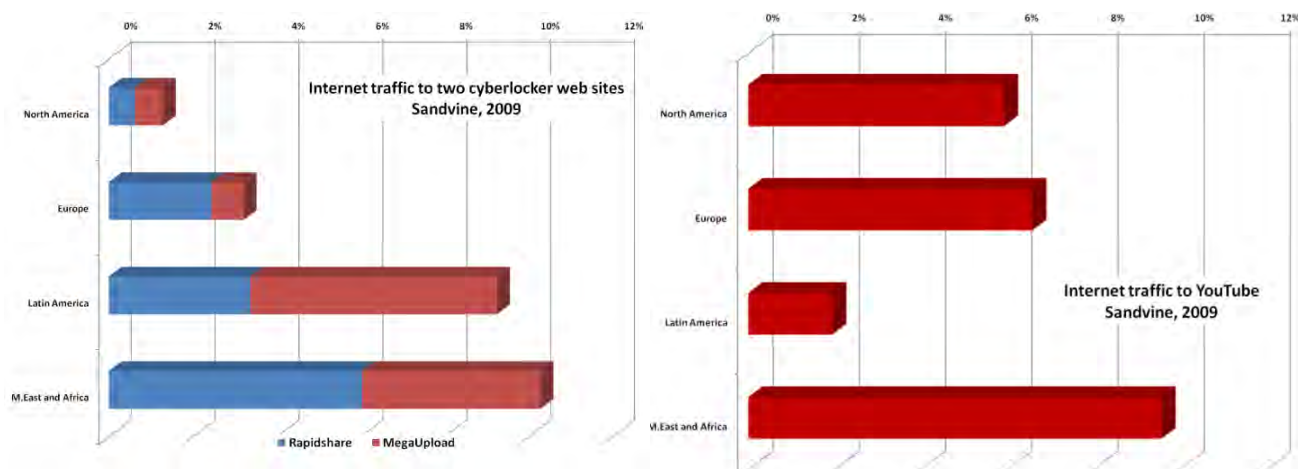


³⁴ Envisional is grateful to the author of the Sandvine study for supplying this additional data.

It is clear that BitTorrent dominates the peer to peer world in the locations monitored by Sandvine: the network makes up more than half of all peer to peer usage detected by Sandvine in each of these four regions and almost all in Europe. There is little eDonkey usage apart from in the Middle East and Africa. This finding likely reflects the countries in which Sandvine has monitoring locations in Europe: eDonkey is believed to be well used in many European countries such as France, Spain, and Italy and it would be difficult to believe that the network is responsible for just 0.3% of internet traffic in these such countries. Ares contributes over 8.6% of traffic in Latin America³⁵ while the four Asian clients comprise no more than 0.3% of all internet traffic in any of the four regions (unsurprising, as data was not supplied for the Asia-Pacific region).

- In **North America**, bittorrent (10.3%) and Gnutella (3.4%) make up almost all of the P2P proportion of overall internet traffic of 14.4% (the lowest of the four regions).
- 90% of P2P use in **Europe** is through bittorrent with the network making up 17.3% of all internet traffic in the region and Gnutella contributing a further 1% of all traffic. As noted above, eDonkey usage is believed to be higher in Europe than shown by Sandvine: other estimates place it at 3-5% of internet traffic.
- **Latin America** also sees more bittorrent usage than any other peer to peer application but Ares comprises 8.6% of internet traffic and 40% of all P2P traffic.
- BitTorrent contributes more to overall internet traffic (21.4%) in the **Middle East and Africa** than anywhere else while there is more P2P use (28.2% of all traffic) in this region than any of the other locations monitored by Sandvine, with eDonkey contributing 4.5% to all internet traffic.

Sandvine also supplied data to Envisional on visitors to the two most popular **cyberlocker web sites**: Rapidshare and MegaUpload. In the North America locations, 1.3% of downstream internet traffic was visits to one or another of these sites (MegaUpload was slightly more popular); in Europe, the figure was 3.2% of total downstream traffic (with Rapidshare much more popular); in Latin America, 9.3% of traffic went to these two cyberlockers (that is more traffic than used by the Ares application and almost as much as bittorrent); while in the Middle East and Africa, these two sites alone were responsible for 10.3% of all downstream internet traffic (with Rapidshare contributing 6% of all internet traffic alone).



³⁵ Including the Caribbean.

Across all four regions, these **two cyberlocker sites alone comprise 5.1% of all downstream internet traffic**. To put this into perspective, it is only a little less than the 6.2% of internet traffic consumed by YouTube worldwide, recognised by Sandvine (and Arbor) as the largest single domain contributor to overall internet traffic. As the second chart above shows, traffic to YouTube also varied from region to region, ranging from 1.9% in Latin America to 9.6% in the Middle East and Africa.

3.2.4 *Summary*

Sandvine's study shows a good level of detail and accompanying analysis. The company's willingness to discuss their approach and provide additional data upon request demonstrates their confidence in the methodology and figures.

However, it is important to remember the relatively small number of monitoring locations from which the data is drawn for some regions (only two locations for Latin America, Asia-Pacific, and the Middle East and Africa) as well as the fact that an overall figure for the amount of data analysed in the study could not be obtained. Further, analysis took place in September, a month when there are few major film releases and the Fall television season in the United States (which tends to produce an increase in the use of P2P networks to download content) is yet to properly begin.

3.3 Arbor Networks: ATLAS Observatory 2009 Annual Report

Monitoring period: July 2007 – July 2009

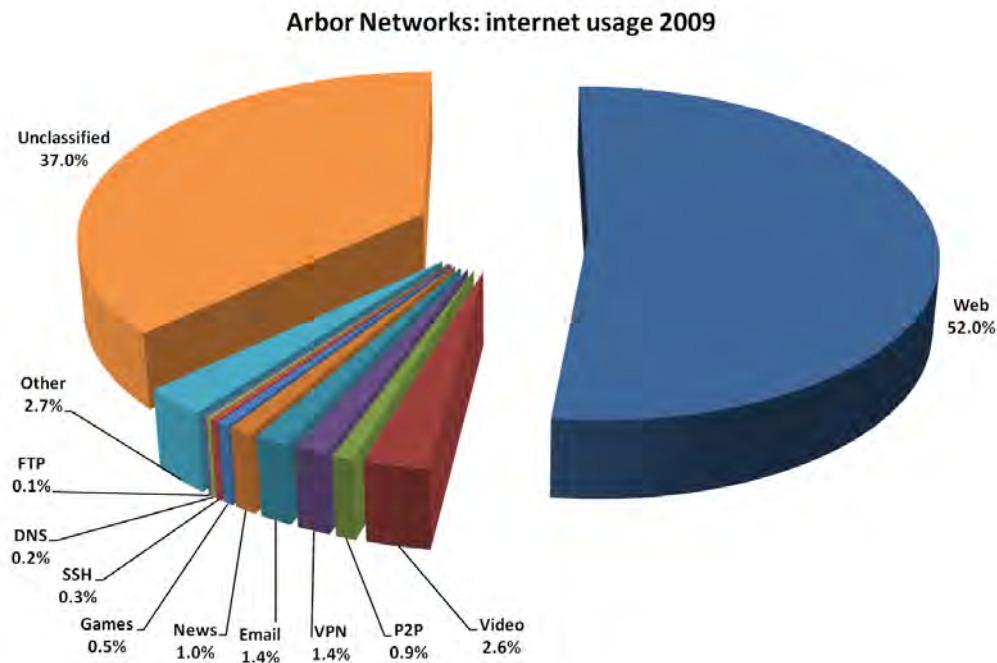
Monitoring locations: 110 deployments across ISPs and Content Providers worldwide (with an emphasis on North America, Europe, and East Asia (including Japan)).

Number of subscribers: unknown.

Amount of traffic monitored: 264 Exabytes of data at a peak rate of 14 Terabytes per second. On average, 9 Exabytes per month. This is by far the largest of all the studies³⁶.

P2P traffic: 0.85% (inspected by port number); 18% (payload inspection of a smaller dataset from 5 ISPs)

Streaming video traffic: 2.64% (estimate of 25% on payload inspection of same smaller dataset)



Other points:

- Streaming video is the fastest growing internet traffic category.
- Google (including YouTube) accounted for 5.5% of all internet traffic in May 2009.
- MegaUpload (a large 'cyberlocker' file host) accounted for at least 0.5% of all internet traffic in May 2009.
- Game console traffic accounted for 0.6% of all internet traffic in May 2009.
- Annual internet traffic growth of 44%.

³⁶ 264 Exabytes = 276m Terabytes = 283bn gigabytes = 64 billion DVDs.

3.3.1 Methodology

Arbor is an established network monitoring and security company. The company's monitoring study is produced in collaboration with authors at the University of Michigan and uses a number of monitoring locations worldwide that employ Arbor's network equipment. These servers sit on the edge of an ISP's network and categorise traffic as it passes with an 'anonymous XML file' containing data reports then sent to central analysis servers.

The Arbor study examines an extremely large amount of content data over a two year period – by far the most substantial data base of any of the four studies. The 264 Exabytes of data is equivalent to 283,500,000,000 Gigabytes – around 64 *billion* full-sized DVDs. The data is taken from a wider spread of monitoring points than others (110, compared to 20 for both the Sandvine and Cisco analyses and just 11 for the iPoque study). A precise breakdown of traffic by region is not outlined but monitoring appears to mainly use locations in North America, Europe, and East Asia (including Japan).

3.3.2 Discussion

The chart above shows the dominance of web-based communication: over half of all internet traffic identified by Arbor took place through the web. Against that, no other identified category was responsible for more than 3% of internet traffic. The video and P2P categories amounted to 3.5% in total.

However, the study is hampered –as the large orange 'Unclassified' segment on the chart makes clear – by issues with detection. In 2009, **37% of the 264 Exabytes of traffic could not be classified** by Arbor. This represents an enormous amount of traffic which could not be identified by the routine monitoring techniques employed by the company. According to subsequent analysis by Arbor, the majority of this unclassified proportion is believed to be either peer to peer traffic or video streaming and downloads, a belief based on analysis of a second and smaller dataset of traffic subjected to more detailed probing.

This second, smaller, dataset was taken from **five consumer ISPs** based in the United States, Canada, Europe, and Asia, though the precise locations and number of subscribers represented are not supplied, and nor is the actual amount of data analysed. This dataset was subjected by Arbor to Deep Packet Inspection (DPI) techniques in an attempt to detect traffic based on the payload of the data. Arbor are confident that their DPI detection is accurate, but detection of peer to peer protocols is not their core business and as such, they may not be catching as much of this traffic as some other companies – certainly, it might be expected that they under-measure P2P than over-measure. However, Arbor were clear in conversation that observations show that there is broad correlation between the overall trends from the smaller DPI-based analysis and the larger, main dataset though without detailed analysis of the smaller dataset this is not possible to confirm.

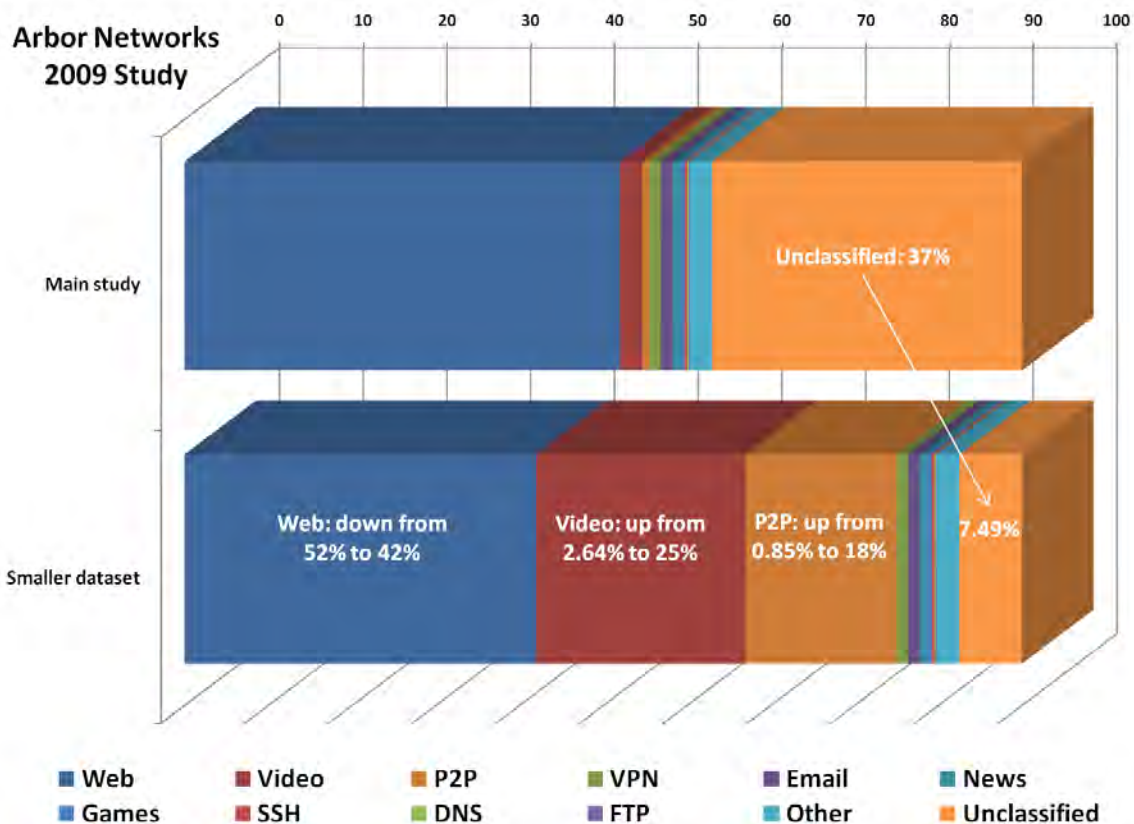
The deeper analysis of the second and smaller dataset via DPI led Arbor to conclude that **"P2P is likely closer to 18%"**. This wording is imprecise and there is no attempt to break down P2P usage by protocol or by region, as

Sandvine manage, for instance³⁷. The dataset was taken from the midpoint of the monitoring (assumed to be during 2008) and no further information is provided on additional changes to P2P traffic after that point.

Similarly, the larger main study appeared to base its analysis of video traffic on older protocols and did not account well for the enormous growth of other transmission methods. A second estimate is made by Arbor through similar DPI analysis of the smaller dataset which estimated video traffic at “**25%+ of all traffic (including 10% of HTTP)**”. Again, the wording is vague and slightly confusing, drawing part of the HTTP traffic to make up the total video proportion.

3.3.3 Accounting for the unidentified data

As noted, **37% of traffic** from the main study was unidentified in 2009. The smaller dataset placed **P2P** usage at 18% rather than 0.85% in the main study, which might account for 17.15% of that unidentified block – leaving 19.85% of unidentified traffic. Some of that may also be accounted for by the **video** data identified by the smaller dataset.



³⁷ The authors do state that P2P varies by region and type of network but this is not elaborated upon.

The smaller dataset identified 25% of data to be video traffic rather than 2.64% in the main study, a difference of 22.36%. However, that figure of 25% for video includes 10% of previously identified HTTP traffic, leaving 12.36% of traffic which can be taken from the unidentified block of traffic.

So if the assumption is made that the smaller dataset portrays similar overall usage patterns to the larger study (and there must obviously be reservations about doing this, given the smaller amount of data and lower regional coverage), calculations then leave **7.49% of traffic unidentified** (37%: 17.15% identified as P2P – 12.36% identified as video).

The chart above shows how the overall usage pattern from the main study significantly changes if the classification of video and P2P usage by the smaller dataset is accepted as correct. While the smaller categories of use (such as email and FTP) remain the same, the three major categories of identified use from the smaller dataset (web, video, and P2P) show large differences.

It is possibly only to speculate what the remaining 'unidentified' amount of traffic might be: given Arbor's primary focus on network monitoring and security, it is possible that some of this data may be peer to peer or other file sharing traffic. Arbor do not mention protocols like those behind 'P2PTV' applications such as PPLive and Sopcast that are often used for video distribution in Asia in their reporting and these may also make up some of the unidentified proportion.

3.3.4 Summary

In summary, the Arbor study, while clearly based on a vast treasure trove of data, is affected by the large amount of that treasure which could not initially be classified. Additional DPI inspection of a smaller dataset provided some additional insight but it is only rational to accept the figures provided for P2P and video consumption in particular as a broad estimate of data usage online rather than a more exact representation.

The issues involved in estimating P2P and video traffic must also affect confidence in figures for the other categories of traffic – although as many of these categories will have changed little over time (for instance, web-based transmissions, email, FTP, and VPN traffic are well established), detection and categorisation should be easier.

3.4 Cisco: 2009 Visual Networking Index Usage Study

Monitoring period: Third quarter of calendar year 2009

Monitoring locations: Over 20 service providers, mostly consumer-based ISPs.

Number of subscribers: 1m

Amount of traffic monitored: Unknown.

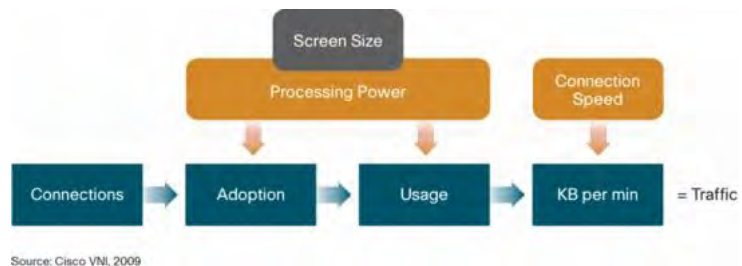
P2P traffic: 38% (worldwide)

Streaming video traffic: 27.7% (worldwide); 30.7% (United States)

Cisco regularly publish data on internet traffic and bandwidth usage within an ongoing research initiative known as the **Visual Networking Index**. The majority of published work within this initiative is based on the interpretation of analyst predictions about the future of internet usage. For these studies, Cisco state:

The core methodology relies on analyst projections for Internet users, broadband connections, video subscribers, mobile connections, and Internet application adoption. Analyst forecasts come from SNL Kagan, Ovum, Informa Telecoms & Media, Infonetics, IDC, Frost & Sullivan, Gartner, ABI, AMI, Screendigest, Parks Associates, Yankee Group, Dell'Oro, and Synergy.

Cisco produces data on the overall use of the internet for the VNI by combining these analyst predictions with an analysis of what are termed 'fundamental enablers' of internet usage such as broadband speed, computing power, and screen size, with the company positing a 'supply-side' aspect to internet usage as well as an end-user demand aspect.



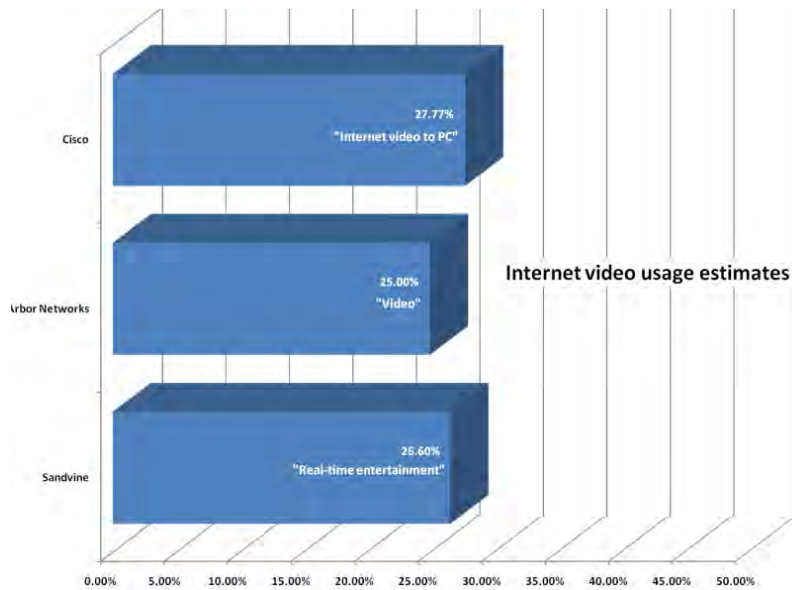
For the purposes of this study, Cisco's analysis is helpful as context but does not provide hard data based on the monitoring of actual internet traffic. However, Cisco also publish a Visual Networking Index **Usage Study** which draws data from over twenty ISPs worldwide serving a total of around 1m subscribers. This uses deep packet inspection to determine the type of data flowing into and out of each ISP.

Unfortunately, the amount of data publicly available from the Usage Study is low and in terms of categorising network traffic, only specific figures for file sharing usage are provided by the company.³⁸ This finds that **38% of global internet traffic can be identified as peer to peer**. The report also finds that "Nearly one-third of all file-

³⁸ The study also provides some data which states that the average broadband connection generates 11.4 gigabytes of Internet traffic per month and that the top 1% of broadband connections are responsible for more than 20% of total Internet traffic.

sharing Internet traffic is non-P2P. Web-based file-sharing, newsgroups, and FTP account for 32 percent of all file sharing traffic.” This means that in total, **55.9% of all internet traffic is what Cisco term file-sharing**. However, the data is not broken down by protocol or type of traffic – for instance, it is not known what proportion of the 38% that is peer to peer file sharing is produced by bittorrent or eDonkey; or how important ‘web-based’ file sharing is, nor exactly which sites are listed under that definition.

Cisco does provide significant detail within the main VNI studies, allowing data estimates to be broken down by country, type of traffic, and for a number of years going forward through a customisable web-based tool. However, as these estimates are based on analyst predictions (and as they differ from that produced within the actual Usage Study (for instance, peer to peer is listed as 31.7% in 2009 rather than 38%), their methodology makes them unsuitable for inclusion in this report. It is worth noting that the estimate for video streaming bandwidth use is very similar to that produced by Sandvine and Arbor, as the chart shows. Cisco defines this as “internet video to PC” and estimate it at 27.7% of all internet usage. This is relatively close to the estimates from Sandvine for ‘Real-time entertainment’ (26.6%) and Arbor’s ‘Video’ category (25.00%) – though again, note that the figures from Sandvine and Arbor are based on actual monitoring data rather than analyst estimates.



3.5 iPoque: Internet Study 2008/2009

Monitoring period: “Two weeks”, varied periods depending on location.

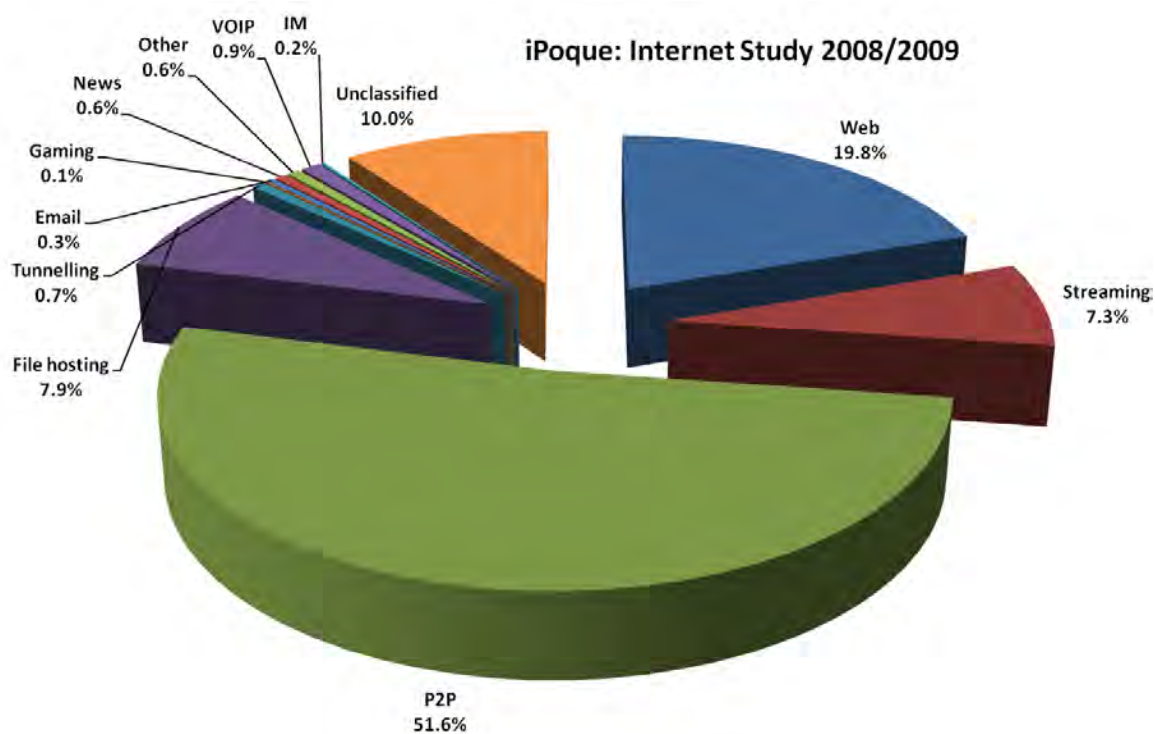
Monitoring locations: 11 monitoring locations; eight ISPs and three universities from eight regions: Africa, South America, Middle East, Eastern, Southern, and Southwestern Europe, Germany. No locations in the United States.

Number of subscribers: 1.1m

Amount of traffic monitored: 1.3 Petabytes (the smallest of the three studies where traffic amounts are known).

P2P traffic: 51.6%

Streaming video traffic: 7.34% (categorised as ‘Streaming’)



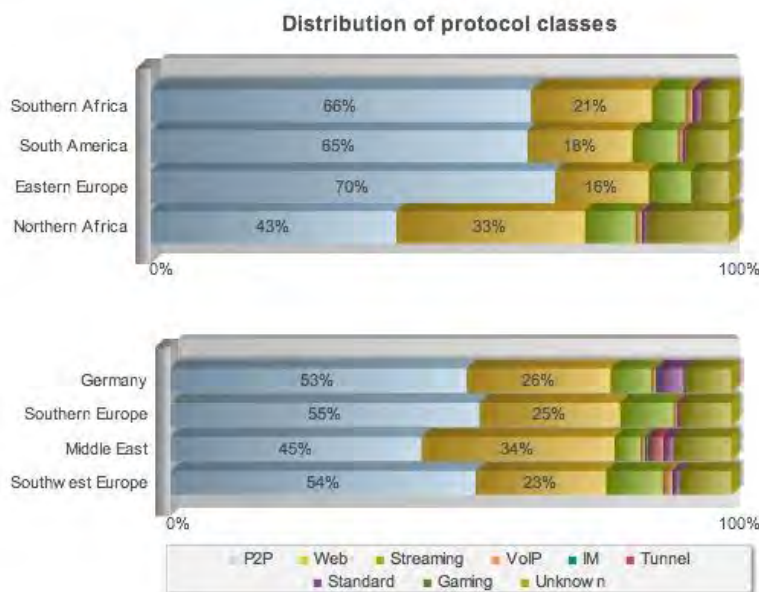
Other points:

- Peer to peer file sharing generates “by far the most traffic in all monitored regions” – from 43% in Northern Africa to 70% in Eastern Europe.
- Peer to peer traffic has dropped slightly as a proportion since their previous 2007 study. BitTorrent is the most popular single protocol.
- File hosting (direct downloads from cyberlockers) has increased to “up to 45% of all Web traffic” in some regions.
- “Rapidshare alone is responsible for 5 percent of the worldwide Internet traffic”.

3.5.1 Methodology

iPoque is a German network monitoring and DPI solutions provider. They claim to be the leading European company in their field. The company has issued 'Internet Study' reports each year since 2007. The 2009 report is detailed in its results and discussion but based on a small amount of traffic³⁹ generated from eleven locations at different (unknown) time periods and which cover a relatively small number of users (1.1m subscribers in total compared to 24m for Sandvine). Each location uses iPoque's PRX Traffic Manager hardware which combines protocol detection with DPI and behavioural traffic analysis.

The eleven locations themselves are scattered around Africa, Europe, and the Middle East, with only one or two locations in each country. Three of the locations are universities where user profiles and bandwidth usage are likely to be significantly different to a consumer ISP. The study notes that the various issues with the data (amount gathered, locations, types of network, time period, number of subscribers) mean that "the results are not statistically representative".



3.5.2 Discussion

The chart above, taken from the iPoque report, again shows the significant variation from location to location of different types of internet usage but also shows substantially different results – particularly for P2P usage – compared to the other three main studies.

³⁹ Arbor's study is based on over 200,000 times as much data.

- P2P is the highest single category in every region, ranging from 45% in the Middle East to 70% in Eastern Europe, far higher than other studies.
- Web use differs from 16% in Eastern Europe to 33% in Northern Africa.
- The 'streaming' category (defined by iPoque simply as audio and video streaming) takes up anything from 5.8% to 10.1% depending on location but does not come close to the one-quarter of internet traffic identified by the preceding three studies.

It is possible that the locations studied by iPoque simply represent areas which show significantly different internet usage to those monitored by Sandvine, Arbor, or Cisco. Previous reports from iPoque have historically shown much higher P2P usage than other monitoring companies: given the commercial focus of the company on the detection of file sharing protocols (and their equipment does appear able to detect an enormous range of protocols), it is also possible that iPoque may be able to detect some traffic which other monitoring companies might miss or be able to more accurately identify protocols. However, the variation is such that this cannot be the sole reason for the differences.

In summary, the iPoque report indicates that peer to peer traffic is very high in most of the monitoring locations from which they have obtained data while streaming is lower than shown in the other three studies. However, it is difficult to generalise from their findings to other locations and, in particular, to other countries. iPoque has good knowledge and capabilities in identifying different protocols but as a study of use in determining bandwidth make-up worldwide and in the United States, the report must be used with caution.

3.6 Focused studies

Two recent academic studies of network usage were also uncovered. Each examine only a single ISP and as such, the ability to generalise from the results will be difficult but each provide some findings worthy of discussion.

3.6.1 Maier et al (2009) - On Dominant Characteristics of Residential Broadband Internet Traffic

Maier et al. studied traffic for 20,000 subscribers from a major European ISP within a single urban area at various points during the second half of 2008 and the first half of 2009.

The study found that HTTP comprised 57.6% of all traffic with bittorrent responsible for 8.5% and eDonkey for 5% of traffic. At least one-quarter of all HTTP traffic carried Flash video with a further 7.6% carrying other video.

Just fifteen domains accounted for 43% of all HTTP traffic (and therefore 26% of all internet traffic). A single cyberlocker / direct download provider was responsible for 15.3% of *all* HTTP traffic (related to this, 14.7% of all internet traffic was in the form of RAR archives, commonly used in cyberlocker or newsgroup downloads).

Rank	Domain	Fraction of Traffic
1	Direct Download Provider	15.3%
2	Video portal	6.1%
3	Video portal	3.3%
4	Video portal	3.2%
5	Software updates	3.0%
6	CDN	2.1%
7	Search engine	1.8%
8	Software company	1.7%
9	Web portal	1.3%
10	Video Portal	1.2%

3.6.2 Erman et al. (2009) - Network-aware Forward Caching

Erman et al. examined internet traffic from 100,000 broadband subscribers from three states from a single broadband provider in the United States. The data analysed was taken at regular points from February 2007 to September 2008. The authors concluded that "HTTP... is increasingly being used to handle most of the Internet's tasks such as distribution of software, updates, patches, and multimedia, and by P2P applications".

- 66% of internet traffic was HTTP; the web is "the workhorse for data delivery"
- Video was a large portion of HTTP and around 22% of all traffic
- 12.3% was P2P (though this portion could be up to 17% given issues with identification)

3.6.3 Layton and Waters, Internet Commerce Security Laboratory (April 2010) - Investigation into the extent of infringing content on BitTorrent networks

This study was on the surface similar to the investigation pursued in Part A of this report into infringing content on bittorrent. The authors gathered data from a range of bittorrent trackers and collated the information, then looked at the most popular 1,000 individual files.

The authors found that 43% of the sample of 1,000 bittorrent swarms was films, 29% was television episodes, and 16.5% was music.⁴⁰ The proportion of torrents infringing copyright was estimated at 89% with no evidence of legitimate usage found in the torrents within the top three categories (film, television, and music).



However, the study had significant methodological flaws and as such, Envisional believes it should not be considered as valid for the purposes of this report.

- The authors chose the most popular 1,000 torrents in terms of **number of seeds** rather than number of downloaders. It is common for fake files or malware to have seed numbers artificially boosted in order to attract downloaders. Little or no work appears to have been done in weeding out the fake files, resulting in a peer count of over 117m seeds across only 1m torrents (compared to just 17m peers in *total* for all 1.8m torrents tracked by PublicBT in Part A).
- There was an issue with **domain pseudonyms** for common trackers. Some of the tracker names used in the data gathering actually point to an IP address for a different (and more popular) tracker altogether⁴¹.
- There are a number of instances where the **reported data** stretches credulity: for instance, at the point of their analysis in April 2010 the most popular file was listed as a pirated version of the film *The Incredible Hulk*. This film was released in 2008 and was not one of the most popular that year, yet the data produced by the authors state that one version for the film had over one million peers, both a level of popularity that is difficult to believe for a film of this age and an absolute number of downloaders that is higher than any single bittorrent swarm ever recorded by Envisional. For example, the number of seeds in the most popular swarm for the final episode of the television program *Lost* – believed to be the highest-seeded bittorrent swarm ever seen – was never above 100,000 at any one time, according to Envisional's own monitoring.

⁴⁰ http://www.icsl.com.au/files/bt_report_final.pdf

⁴¹ For instance, the tracker address "tracker.ilibr.org" points to the PublicBT tracker: a query to the ilibr.org tracker is actually sent to the PublicBT tracker instead. With both the ilibr tracker and the PublicBT tracker included in the data gathering, the same information is being gathered twice. Further, two versions of the ilibr.org tracker are included on two different ports - yet these both point to PublicBT and will end up querying the same tracker twice (the port numbers make no difference in this aspect).

3.7 Summary: Bandwidth Usage

As the preceding discussion makes clear, navigating through studies of internet traffic in order to attempt some level of consensus is challenging. With no established or accepted methodology, classifications, or measurement techniques, the analyst depends on the detail provided in each study to assign confidence and gain understanding.

Each of the four main studies discussed have methodological issues of a greater or lesser extent.

- **Sandvine's** report is detailed but the amount of traffic on which the analysis is based is not provided. Given that the focus is upon three weeks of analysis across 24m ISP subscribers, the data volume should be significant. Further, the methodology is outlined clearly and the company was also willing to discuss their approach and send further data when requested.
- The **Arbor** study is based on a volume of data which dwarfs all other studies but detection is poor and while a smaller dataset is analysed to allow more precise measurement of certain sectors, confidence is obviously affected.
- **Cisco** provides only a few data points. Their main VNI reports provide granular data for a wide range of applications and countries yet rely on analyst predictions rather than data measurement. The focus is much more on predicting network growth than on detailing traffic for a particular time period.
- **iPoque's** report relies on a limited sample of data from varied dates across a small range of monitoring locations in less developed internet markets.

Apart from Arbor who do not analyse traffic in this manner, all studies show significant regional variation. Internet usage in North America is clearly not the same as in Latin America or Europe or Asia. The variations shown for instance by iPoque across monitoring locations in the same small region demonstrate that there can be large variations between countries (and likely within countries, also). Envisional's own monitoring data for networks like bittorrent and eDonkey show differences between countries in usage of those protocols.

With the limitations of each study in mind, it does seem possible to generate some broad conclusions and estimates about internet traffic using the data provided.

3.7.1 The importance of the web

- Standard, daily, routine **web browsing** – to Google, Facebook, the BBC, Wikipedia, Twitter, Amazon, eBay, Flickr, blogs, forums, and so on – is responsible for around **one-third of all internet traffic**. It may be difficult to be more precise than this: so many applications and sites employ the web for distribution or storage of content that categorisation becomes difficult. Sandvine and Cisco appear to ensure that most web traffic which is not web-page based (such as video streams, file hosting downloads, and so on) are



Web: 33%

categorised separately but the two studies diverge significantly over how much traffic is then left: Sandvine posits 33.7%; Cisco's VNI study estimates just 18.2% (a figure which also includes email and instant messaging data). Arbor finds that 42% of internet traffic is 'Web' while iPoque estimates anywhere from 16% to 34% depending on location (with

this figure including file hosting sites). The smaller Maier and Ermann studies find around 35% of traffic to be non-video HTTP traffic. For this report, the amount of web usage is held to be 33% of all internet traffic.

- In the **United States**, the maturity of the web and its place as home to so many applications which have extended the use of the web – Google, YouTube, Facebook, Twitter, and so on – mean that relative web use in the US may be higher than that observed worldwide. Both Sandvine and Cisco (the only two of the four studies to analyse the US or North America separately) report or estimate slightly higher web use in the country.
- Beyond everyday web browsing, there are two other areas of web-based traffic which should be considered separately: **streamed video** (and to a lesser extent, audio); and **file hosting** or cyberlockers.
 - **Video content**, particularly streamed video, is one of the major components of internet traffic, with much of it being transmitted through or sourced from HTTP communication. Three of the studies reach a broad level of consensus on the level of internet traffic which features streamed content: Sandvine's 'Real-time entertainment' category, Cisco's 'Internet video to PC' estimate, and Arbor's simple 'Video' category all place web-based video viewing at around **25%-28% of traffic** (and is assumed to be 26.5% for the purposes of further analysis in this report). Sandvine's category includes audio-only streams and Arbor's category is hardly defined at all but the figures are relatively close in agreement. This is an area where the iPoque study shows considerable difference to the other three reports. It is possible that streamed video is less important in the locations where their measurement technology is based but without further detail on the countries from which iPoque are reporting, this can only be speculation.

Video: 25-28%

On-demand video content appears to be consumed more highly in the **United States** (the home of YouTube and many other online video hosts) than in other regions: ComScore reported that over 173m internet users in the US watched more than 32bn videos during January 2010 alone, significantly higher figures than for users in Germany and France, for instance. With this in mind, an estimate for video usage in the United States as comprising 27%-30% of internet traffic can be made.

- The use of central web-based **file hosting sites or cyberlockers** such as Rapidshare and MegaUpload can be significant depending on country. These sites seem to be more heavily used in Europe and less developed internet markets (such as the Middle East and Africa) than they are in North America. Sandvine estimate that cyberlockers are responsible for around 5.3% of all internet traffic, and this should be seen as a minimum – the company's list of sites included in the 'Storage and backup' category is far from exhaustive for cyberlockers. However, no other cyberlockers are as large as Rapidshare and Sandvine provides detailed traffic analysis for that site and for MegaUpload. Thus while actual cyberlocker usage may be higher than Sandvine's figure, it is likely not much higher. iPoque believe that Rapidshare alone contributes 5% of all traffic and that cyberlockers overall are responsible for 7.9% of traffic though this comes from countries where cyberlocker usage appears to be relatively high. Cisco do not delineate this area specifically but do estimate 'non-P2P' filesharing (web-based file sharing, newsgroups, and FTP) at around 19%. It is reasonable to assume that most of this non-P2P filesharing will be from cyberlockers as newsgroups and FTP are shown in other studies to be around

*File hosts /
cyberlockers: 7%*

1% of all internet traffic and little more. As with their estimate for peer to peer usage (see below), Cisco are therefore estimating a much higher level of cyberlocker usage.

Arbor are fairly quiet on this issue, stating only that MegaUpload was found to be responsible for around 0.6% of all internet traffic in early 2009.

Analysis of the overall data available leads to a cautious estimate that central file hosts like cyberlockers are responsible for around **7% of internet traffic**.

Data from Sandvine – the only source of information on this area – show relatively low usage of the two main cyberlockers for users from North America. Given this, an estimate of cyberlocker usage for the United States of **3%** is acceptable.

3.7.2 Peer to peer remains significant

- **Peer to peer applications** have traditionally been considered to take up a very large amount of internet traffic: studies from 2005 found that more than half of all internet traffic used peer to peer. That may have been correct at that time but as noted above, there has since been a resurgence of the importance of the web to internet users at the same time as the internet has become increasingly a video-based medium. This is not to say that peer to peer traffic is declining in absolute terms.

Determining how much internet traffic is peer to peer is more difficult. The proportion varies from study to study and, within those studies, from region to region, but it is likely that at least 20% of all internet traffic comes from peer to peer applications. Sandvine's figure is 20.4% worldwide and this may be slightly low. The list of P2P protocols included in their study is not exhaustive, though does include the major networks. However, both iPoque and Cisco place P2P usage much higher: the former at over 51% and the latter at 38%. iPoque's figure can only be taken as evidence of P2P usage in the particular locations they monitor. Cisco's figure is from a relatively small sample of 1m subscribers but accords with the higher figure they estimate from analyst predictions.

*Peer to peer:
25%*

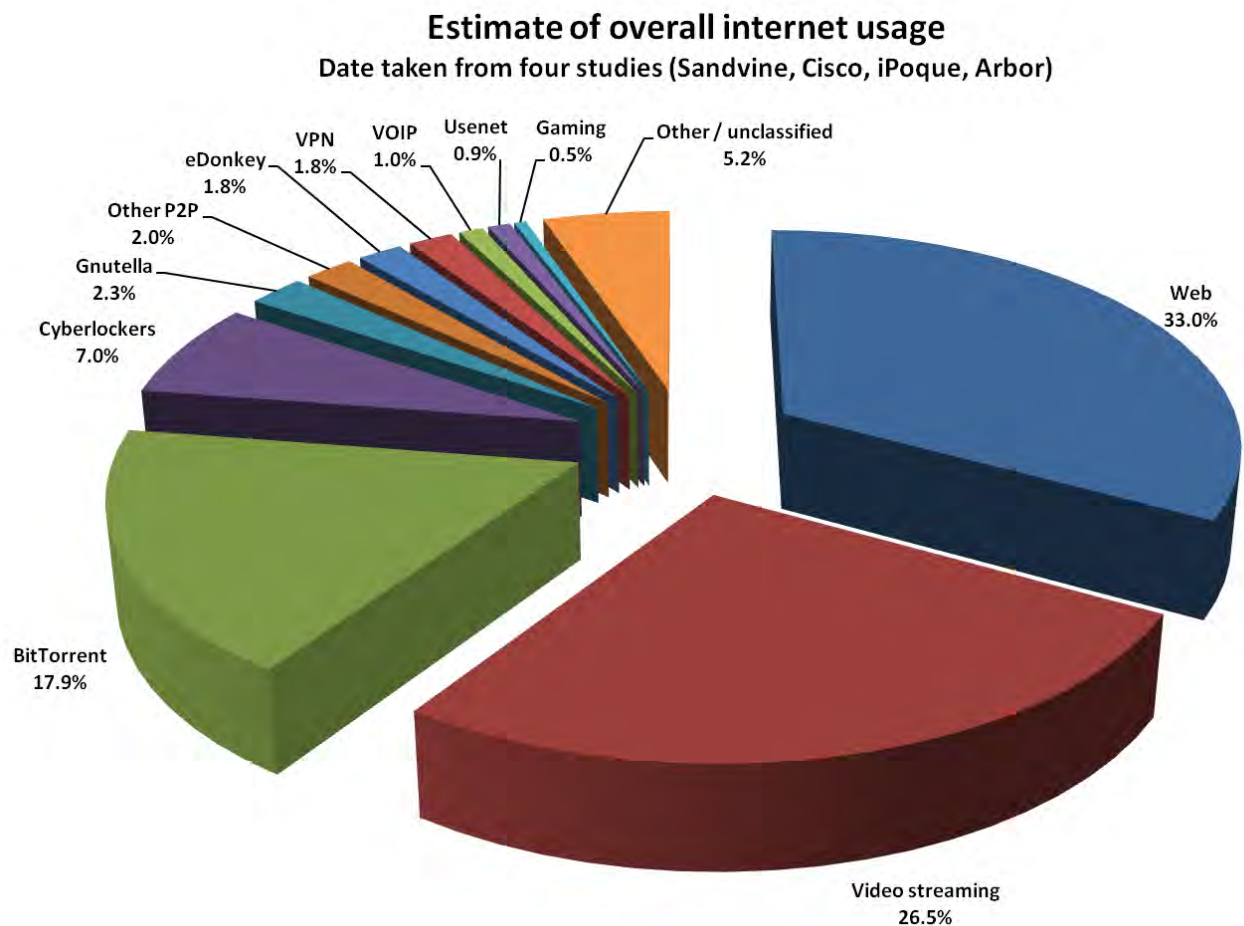
Given these issues, this analysis estimates P2P usage worldwide at **25%** of all internet traffic. On this reading, bittorrent uses around 17.9% of all internet bandwidth.⁴²

- The **United States** appears to be one of the lowest relative users of peer to peer worldwide: Sandvine measure aggregate (downstream and upstream) peer to peer traffic at 18.5% in North America and 14.6% for downstream, mostly through bittorrent. Similarly, Cisco's estimate falls from 31.7% for worldwide P2P usage to 23.9% for the United States alone. There is thus less of a gap between the two studies to reconcile. Assuming US P2P usage to be around **20% of internet traffic** seems reasonable with bittorrent at 14.32% and other peer to peer traffic accounting for just over 5%.

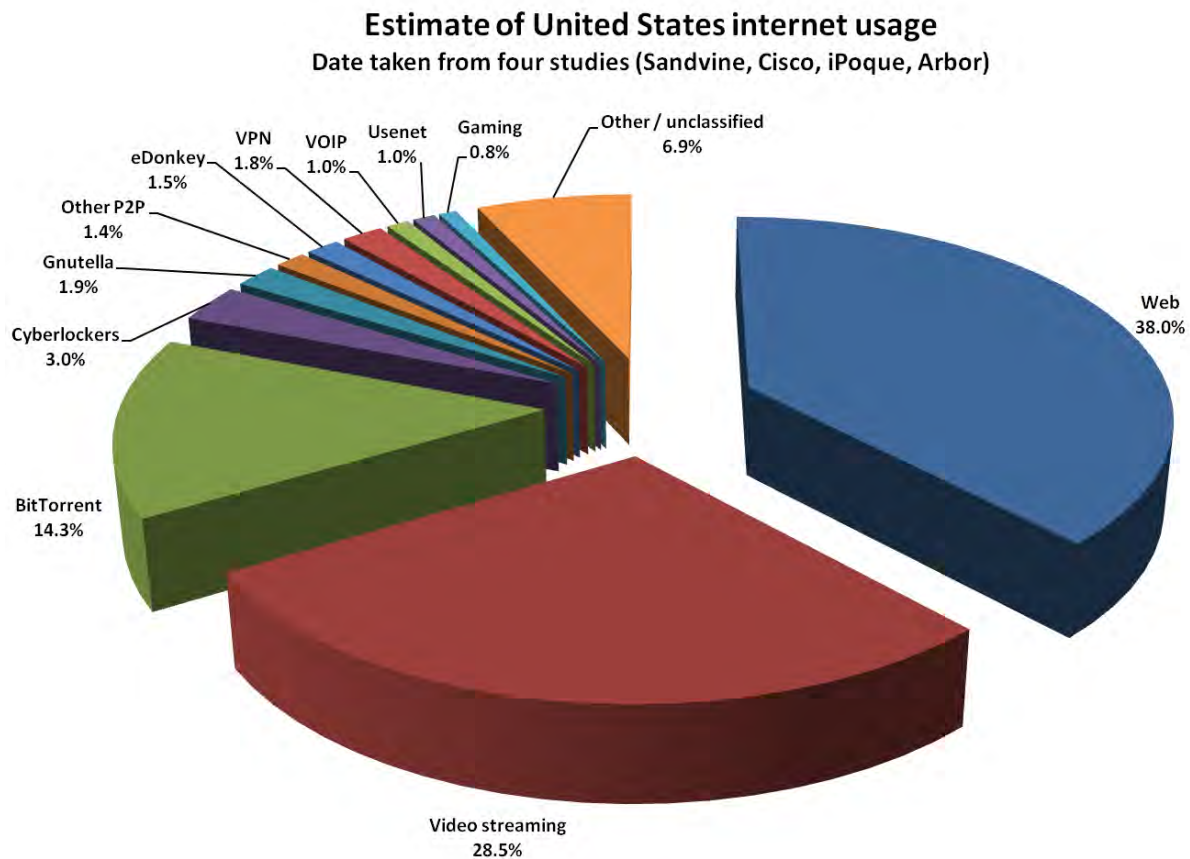
⁴² Only Sandvine provide an overall figure for the amount of network traffic for which bittorrent is responsible: 14.1% (or 71.6% of all peer to peer traffic). If Sandvine's peer to peer estimate of 20.4% is taken as slightly low and the figure of 25% is assumed for all peer to peer data, then the overall figure for bittorrent would be extrapolated to 17.89% of all internet traffic.

3.7.3 Overall estimate

The chart below uses Envisional's own analysis experience and internet intelligence to draw together the four monitoring studies in order to produce an overall estimate for internet bandwidth usage. Web traffic and video streaming (most of which takes place through the web or via HTTP) makes up almost 60% of all bandwidth. BitTorrent provides another 17.9% with peer to peer overall contributing 25% of internet bandwidth. Areas of internet usage such as VPN tunneling, voice over IP, and gaming, are estimated by each of the four monitoring companies to contribute much smaller amounts of overall bandwidth.



In the United States, the higher relative use of the web and video streaming means that these two components are responsible for two-thirds (66.5%) of all bandwidth. BitTorrent usage is slightly lower at 14.3% with other peer to peer protocols contributing a further 5.7% of internet bandwidth. Cyberlocker usage is estimated to be lower in the US than elsewhere in the world, while Gaming and Usenet consumption is very slightly higher.



Part C of this report brings together these overall estimates from Part B with the analysis of common piracy arenas found in Part A to provide an estimate of the amount of internet traffic overall which is believed to be infringing.

4 Part C: Drawing the data together

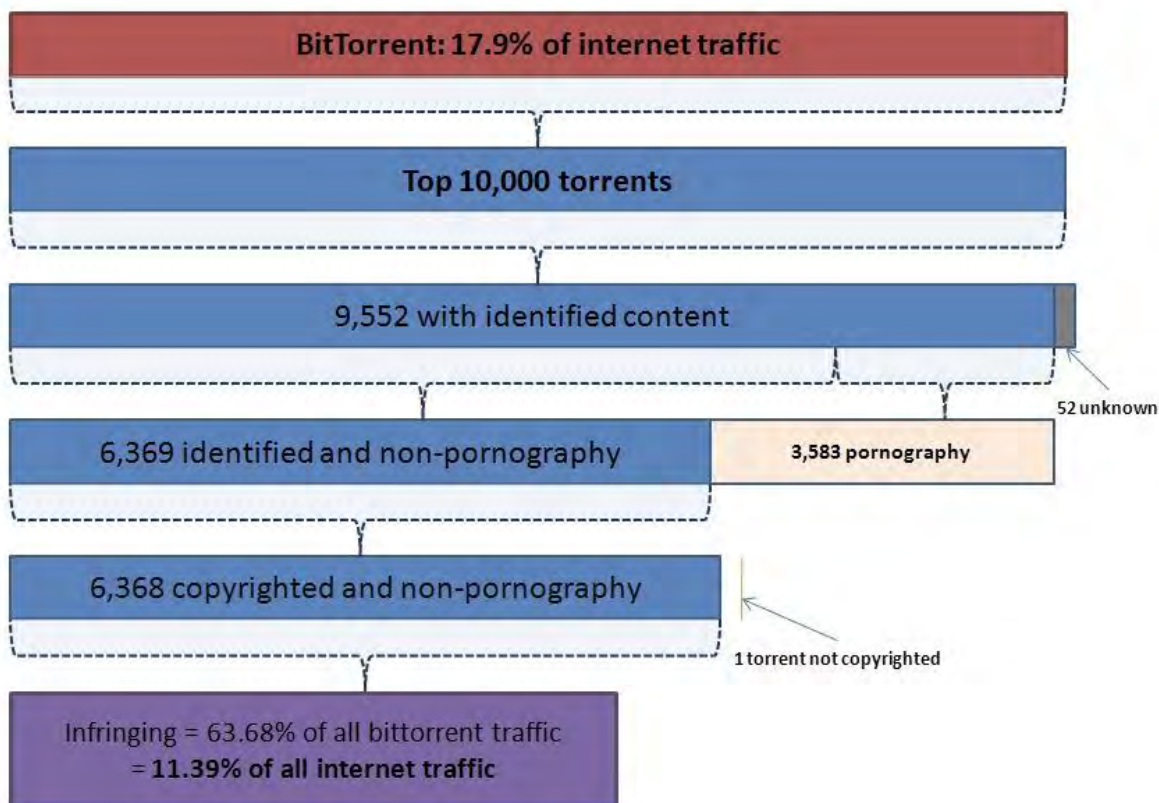
4.1 Introduction

Part A of this report examined a range of common internet arenas where pirated activity is often found and attempted estimates of the level of infringing activity found within each. Part B critically assessed four studies that attempted to determine the amount of overall internet bandwidth used by different protocols and types of content.

This final part of the report brings together these two parts in an attempt to provide an overall estimate for the amount of all internet traffic likely to be infringing. Each of the common piracy arenas examined in Part A will be summarised in turn.

4.2 Estimates of infringing use

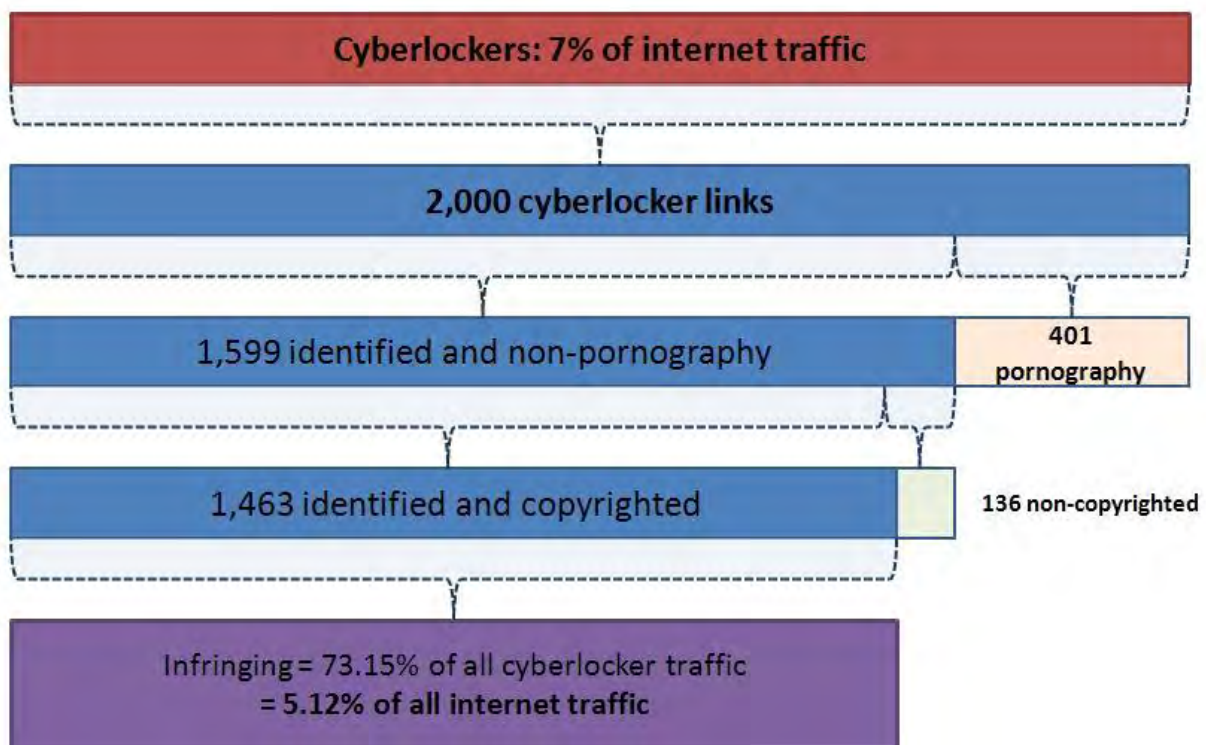
4.2.1 BitTorrent



The chart for bittorrent starts with the estimated 17.9% of internet bandwidth which is believed to be bittorrent. The amount of that bandwidth deemed to be infringing is estimated by reference to the analysis of the most popular 10,000 torrents held on PublicBT (found in Part A of this report). 63.68% of these torrents were found to be infringing and not pornography. This means that 63.68% of the internet bandwidth consumed by bittorrent can be estimated to be of infringing content, resulting in a final estimate that **infringing use of bittorrent is responsible for 11.39% of all traffic on the internet.**

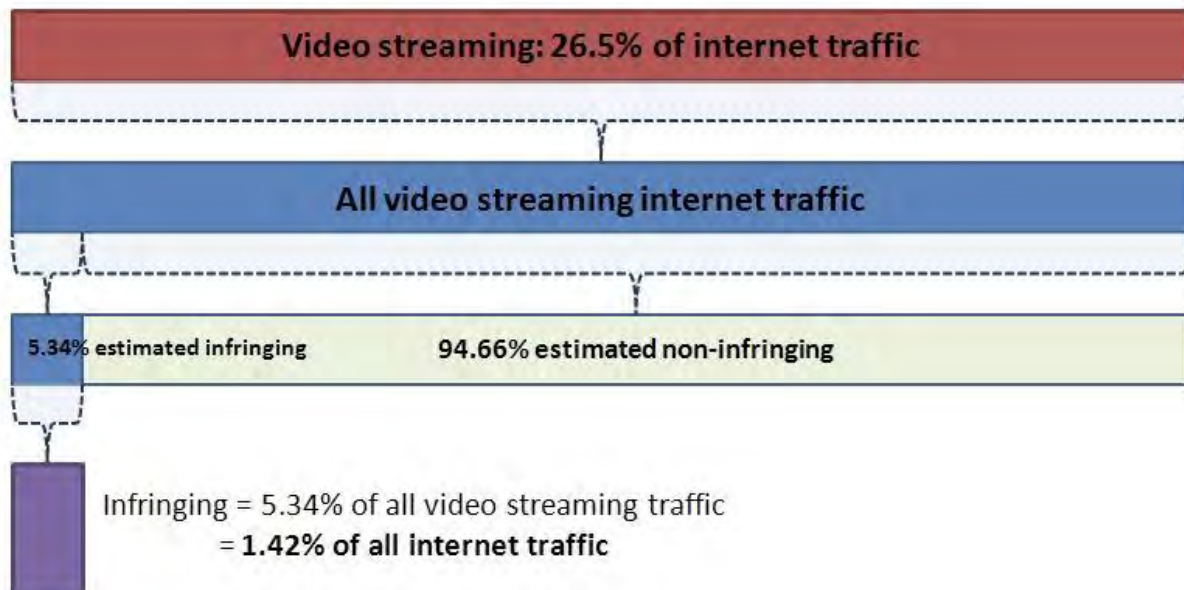
4.2.2 Cyberlockers

Cyberlockers are estimated to be responsible for 7% of all internet traffic. The estimations produced in Part A lead to a belief that around 73.15% of traffic to cyberlockers is related to infringing content. With an estimated overall internet bandwidth usage of 7% down to cyberlockers, this leads to an overall estimate for **infringing use of cyberlockers as 5.12% of all internet bandwidth.**



4.2.3 Video streaming

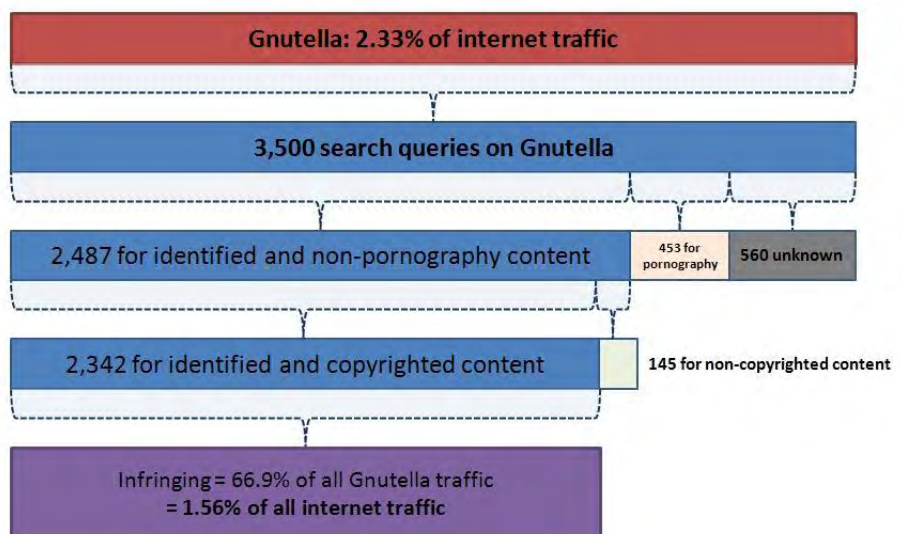
As Part A showed, the largest proportion of video streaming usage is legitimate and non-infringing. The studies discussed in Part B also demonstrated that video streaming traffic is the fastest growing area of internet consumption and is already responsible for more than one-quarter of all internet usage. As such, despite only 5.34% of all video streaming traffic estimate as infringing, this still amounts to **1.42% of all internet traffic**.



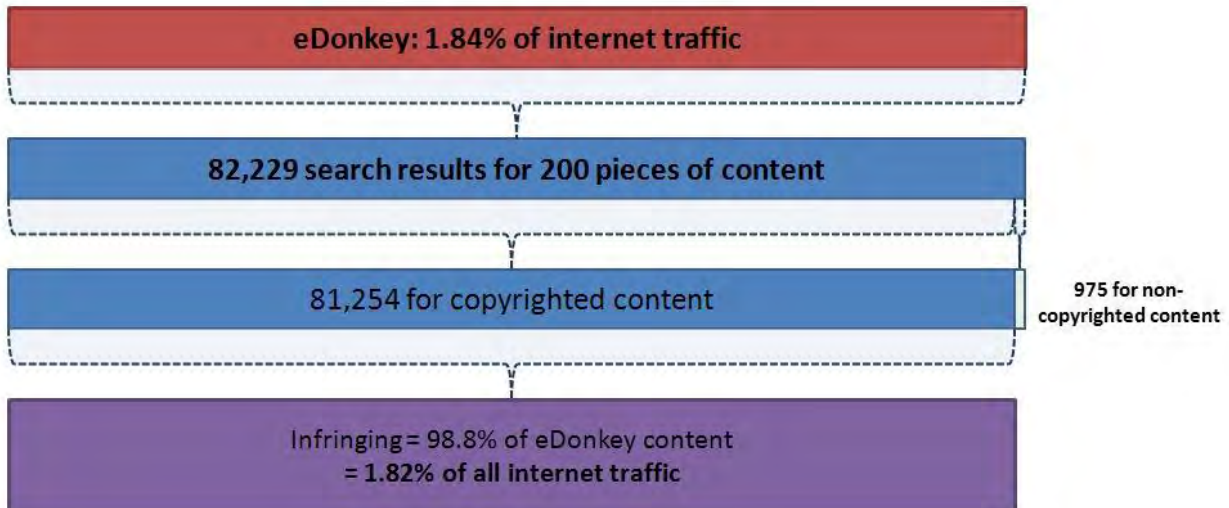
4.2.4 Other piracy arenas

Three other common piracy arenas were analysed in Part A: Gnutella, eDonkey, and Usenet.

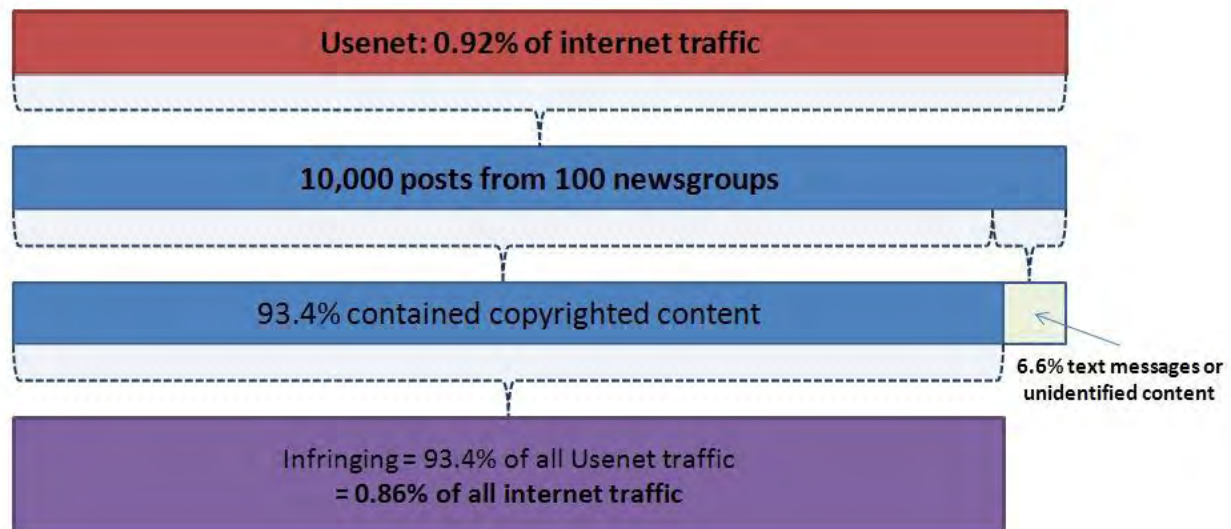
Gnutella is believed to be responsible for around 2.33% of internet traffic worldwide. With 66.9% of content searched for on the network estimated to be infringing and non-pornography, this leads to an estimate of **1.56% of internet traffic contributed by infringing content on Gnutella**.



eDonkey is heavily used in continental Europe, though it has declined in usage over the last two to three years after a series of successful anti piracy actions. The estimate in Part A is that 98.8% of eDonkey content is infringing. With 1.84% of internet traffic believed to be eDonkey, this would mean that **1.82% of all internet traffic is infringing content on eDonkey.**



Part A estimated the proportion of **Usenet** content that was infringing at 93.4%. The best estimate possible from the four studies in Part B found that Usenet made up 0.92% of all internet traffic. This would produce an overall estimate for the amount of infringing internet traffic from Usenet of 0.86%.



Other P2P or file sharing networks also exist which are not explicitly covered within this research, such as Ares, DirectConnect, Kad (a sister network to eDonkey), Gnutella2 (used by clients like Shareaza), and MP2P (used by Piolet and Blubster), for instance. The four monitoring studies lead to an overall estimate for peer to peer usage other than the networks already discussed above of **2.02%**.⁴³ It will be assumed that infringing use of these networks is similar to the average infringing use of the networks analysed here in more detail: 78.94%. This would lead to an estimate of **overall internet use contributed by infringing content on these networks of 1.6%**.

Other types of internet traffic may also be used for infringing purposes. For instance, unauthorised copyrighted content might flow across VPN traffic and some VPN services like Relakks in Sweden exist primarily to hide file sharers from detection. Infringing content might also be transferred across email or be downloaded from normal web sites or blogs, for instance – though this would usually be small pieces of content such as music files rather than anything larger. However, estimating the size of this infringing traffic is extremely difficult, though experience means that the amount is likely to be small relative to the overall amount of bandwidth estimated for each type of traffic. As such, infringing content in these other areas is discounted for the purposes of this report, though this should not be taken as an indication that they are not used for the purposes of infringement.

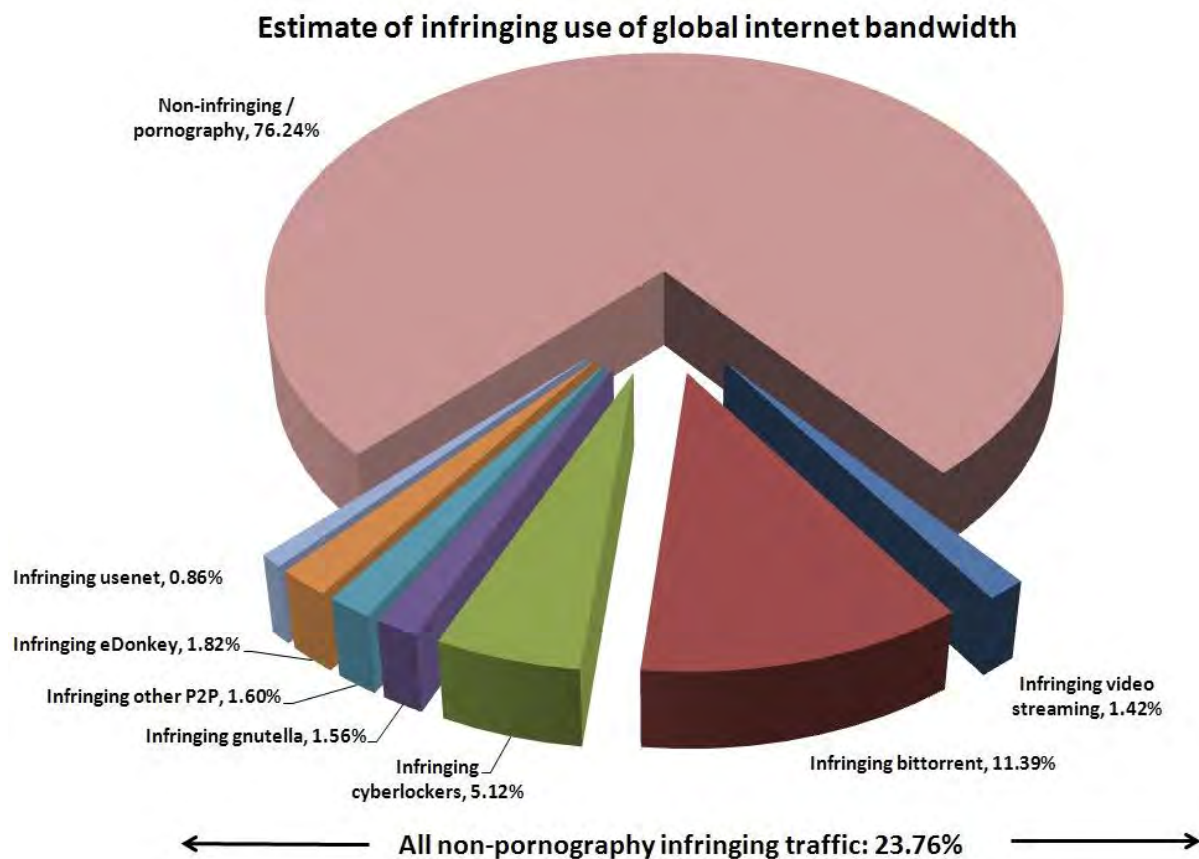
⁴³ A figure derived by taking the overall estimate for peer to peer traffic and subtracting the networks already identified (bittorrent, eDonkey, and Gnutella, for instance).

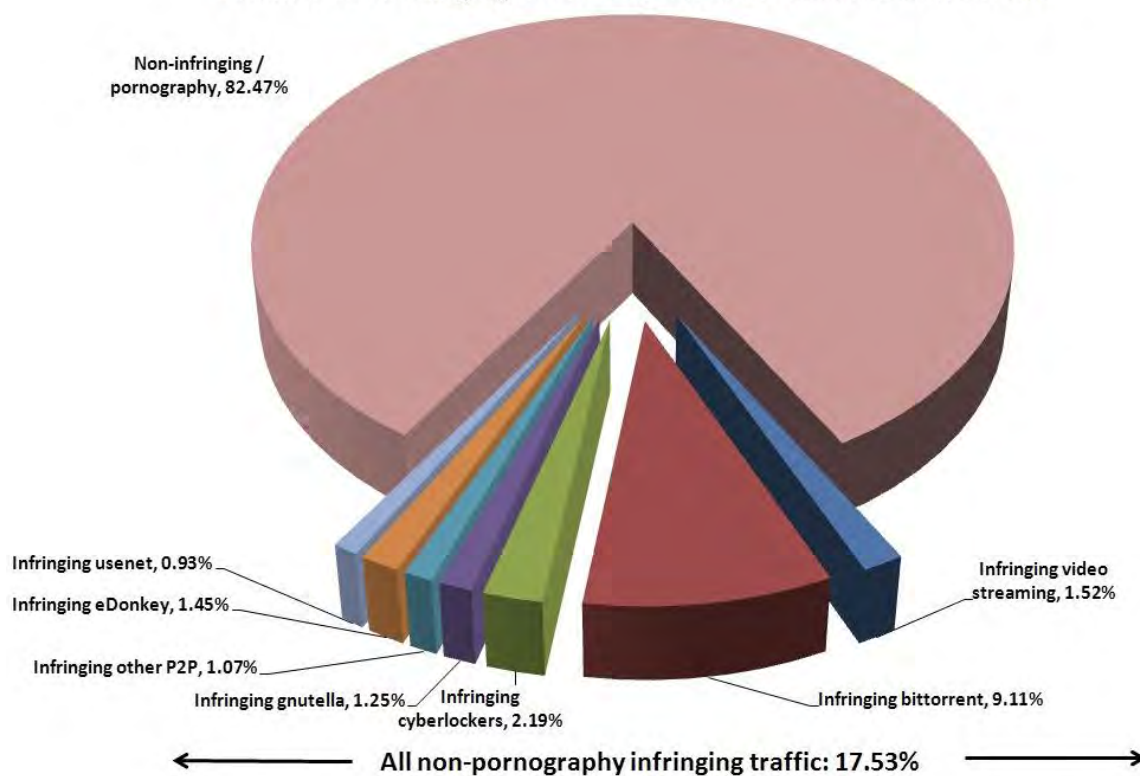
4.3 Summary

This report attempts to produce an estimate for the proportion of traffic which crosses internet that infringes copyright. Using studies of overall internet usage and analysis of common arenas through which content is transferred on the internet, the report finds that it is possible to calculate that a minimum of **23.76% of all internet bandwidth is devoted to the transfer of infringing and non-pornographic content.**

In the United States, the transfer of infringing and non-pornographic content is estimated to be responsible for a minimum of **17.53% of all internet bandwidth.**

The charts below show the overall estimate for the amount of global internet bandwidth which is believed to be infringing (and not pornography) and the overall estimate for the amount of United States internet bandwidth.



Estimate of infringing use of United States internet bandwidth

These estimates must, obviously, be issued with numerous caveats, both about the quality and accuracy of the data offered by the monitoring companies which estimate overall internet usage and about the ability to precisely quantify the proportion of infringing content on each arena of the internet. Methodological issues abound in both areas. Yet even given the limitations of the data available, Envisional believes that the estimates produced in this report are more accurate than any that have been published before. This report draws together the data in a way that allows, for the first time, the organisations which can help shape the ways in which users interact and obtain content to understand how much of the internet is devoted to the distribution and consumption of infringing material.

Piracy Intelligence

Envisional Ltd



Exhibit 9

to

Plaintiff's Response to Order to Show Cause - CV 10-04472 BZ

On The Cheap, LLC DBA Tru Filth, LLC v. Does 1-5011, Case No. CV 10-04472 BZ

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

VOLTAGE PICTURES, LLC,

Plaintiff,

v.

DOES 1-5,000,

Defendants.

Civil Action No. 10-0873 (BAH)
Judge Beryl A. Howell

MEMORANDUM OPINION

Pending before the Court are motions to dismiss, quash, and for protective orders filed by 119 putative defendants.¹ These individuals have yet to be named as defendants in this case, but

¹ Eighty-one individuals have filed motions representing that they are putative defendants in the instant lawsuit, but have not provided the IP addresses listed in the plaintiff's Complaint that are allegedly associated with their computer use. *See* Jeff Kowalski, ECF No. 9 (No IP address listed); Margaret Wenzek, ECF No. 15 (No IP address listed); Audrey Kalblinger, ECF No. 16 (No IP address listed); JoNeane Key, ECF No. 18 (No IP address listed); John Doe, ECF No. 18 (No IP address listed); Nicole G. Lipson, ECF No. 18 (No IP address listed); Kenneth G. Kupke, ECF No. 18 (No IP address listed); Delmar R. Towler, ECF No. 18 (No IP address listed); Richard L. Stellah, ECF No. 18 (No IP address listed); Darcie Dikeman, ECF No. 21 (No IP address listed); Jason Brittan, ECF No. 28 (No IP address listed); Sherry Porter, ECF No. 29 (No IP address listed); Michael B. Parker, ECF Nos. 31, 110 (No IP address listed); James Kane, ECF No. 32 (No IP address listed); Ben Hatch, ECF No. 38 (No IP address listed); Sandra Dockery, ECF No. 39 (No IP address listed); Colin Quennell, ECF No. 40 (No IP address listed); Raghbir Singh, ECF No. 42 (No IP address listed); Arthur B. Cutting, ECF No. 44 (No IP address listed); LaMarr M. Jones, ECF No. 46 (No IP address listed); Adam Delgado, ECF No. 49 (No IP address listed); Karen Eiriz, ECF No. 50 (No IP address listed); Lucy A. Marsh, ECF No. 53 (No IP address listed); Michael Koenig, ECF No. 54 (No IP address listed); Cheryl A. Lobo, ECF No. 56 (No IP address listed); Randall J. Azbill, Sr., ECF No. 57 (No IP address listed); John T. Kraye, ECF No. 58 (No IP address listed); Joseph M. Luria, ECF No. 59 (No IP address listed); Cameron J. Kennedy, ECF No. 60 (No IP address listed); Shey Davis, ECF No. 61 (No IP address listed); David Allan Doll, ECF No. 62 (No IP address listed); Jonathan D. Coleman, ECF No. 63 (No IP address listed); Joseph M. Orovic, ECF No. 65 (No IP address listed); Rowena K. Cruz, ECF No. 66 (No IP address listed); Miriam Adelson, ECF No. 67 (No IP address listed); Antonio R. Hinton, ECF No. 68 (No IP address listed); Judy Collins, ECF No. 69 (No IP address listed); Aran Bedarian, ECF No. 71 (No IP address listed); Nick Hartmann, ECF No. 73 (No IP address listed); Jomy Joseph, ECF No. 74 (No IP address listed); Jonathan T. Payne, ECF No. 75 (No IP address listed); Carman I. Goodrich, ECF No. 76 (No IP address listed); John C. Jacobson, ECF No. 77 (No IP address listed); Ruth Shih, ECF No. 78 (No IP address listed); Sean E. Ringle, ECF No. 79 (No IP address listed); Simone J. Johnson, ECF No. 80 (No IP address listed); Jordan C. Neptune, ECF No. 81 (No IP address listed); Warren M. Gehl, ECF No. 82 (No IP address listed); Eric M. Miller, ECF No. 83 (No IP address listed); Richard T. Holbrook, II, ECF No. 84 (No IP address listed); Darren Choong Sik Hng, ECF No. 85 (No IP address listed); Todd D. Merrifield, ECF No. 86 (No IP address listed); Leanne Ferguson fka Leanne Brogdon, ECF No. 94 (No IP address listed); Amelia Cardenas, ECF No. 95 (No IP address listed); Amanda J. Quast, ECF No. 96 (No IP address listed).

claim to have received notices from their Internet Service Providers (hereinafter “ISPs”) that plaintiff Voltage Pictures, LLC seeks their identifying information in connection with allegations in the Complaint that certain IP addresses used a file-sharing program called BitTorrent to download and distribute illegally the plaintiff’s copyrighted movie *The Hurt Locker*. These 119 putative defendants have filed motions and letters seeking to prevent disclosure of their identifying information and otherwise to secure dismissal from the lawsuit. For the reasons set forth below, the putative defendants’ motions to quash, dismiss, and for protective orders are denied.

I. BACKGROUND

On May 24, 2010, plaintiff Voltage Pictures, LLC filed a Complaint against unnamed individuals who allegedly used a file-sharing protocol called BitTorrent to illegally infringe plaintiff’s copyright in the motion picture *The Hurt Locker*. Compl. ¶ 3, ECF No. 1. Given that the defendants in this case were unidentified at the time the plaintiff filed its Complaint, on June 25, 2010, the Court granted the plaintiff leave to subpoena ISPs to obtain identifying information for the putative defendants. Minute Order dated June 25, 2010 (Urbina, J.).

Since the Court approved expedited discovery, ISPs have provided identifying information

listed); Randy L. Morton, ECF No. 97 (No IP address listed); Morris Carrejo, ECF No. 99 (No IP address listed); Charles Ellsworth, ECF No. 100 (No IP address listed); Nanci Lam, represented by Michael S. Lee, Esq, ECF No. 101 (No IP address listed); Anita M. Dorrance, ECF No. 104 (No IP address listed); Syed Mobeen, ECF No. 105 (No IP address listed); Alan Stowers, ECF No. 107 (No IP address listed); Shani Myers, ECF No. 108 (No IP address listed); Darryl Godfrey, ECF No. 109 (No IP address listed); Justin Solem, ECF No. 112 (No IP address listed); Adam Owensby, ECF No. 118 (No IP address listed); Kathryn Lanier, ECF No. 119 (No IP address listed); Erik E. Johnston, ECF No. 121 (No IP address listed); Leigh Norris, ECF No. 126 (No IP address listed); Michael Scott Davis, ECF No. 127 (No IP address listed); Matthew Alan O’Connell, ECF No. 128 (No IP address listed); Kathleen Gonzales, ECF No. 129 (No IP address listed); Neel N. Patel, ECF No. 130 (No IP address listed); Nancy Schwarz, ECF No. 131 (No IP address listed); Matthew J. Selck, ECF No. 132 (No IP address listed); Von R. Arnst, ECF No. 133 (No IP address listed); Freightmen International, ECF No. 140 (No IP address listed); Adrian Taylor Tuia, ECF No. 134 (No IP address listed); Guntars Rizijis, ECF No. 137 (No IP address listed); Chris Queen, ECF No. 138 (No IP address listed). The Court therefore has no way of verifying that these individuals are indeed potential parties in this lawsuit. Regardless, however, the defenses and arguments they assert are identical to those proffered by other putative defendants.

for the putative defendants in response to the plaintiff's subpoenas on a rolling basis.² Prior to providing the plaintiff with a putative defendant's identifying information, however, the ISPs sent notices to the putative defendants informing them of their right to challenge release of their information in this Court.³ On April 4, 2011, the Court directed the plaintiff, *inter alia*, to dismiss the putative defendants that it did not intend to sue. Order Granting In Part Pl.'s Mot. Extension of Time to Name and Serve, Apr. 4, 2011, ECF No. 120. On April 15, 2011, the plaintiff voluntarily dismissed 557 putative defendants for whom it had received identifying information but did not intend to sue in this Court. Pl.'s Notice of Voluntary Dismissal, Apr. 15, 2011, ECF No. 125. None of the putative defendants with pending motions were dismissed. *Id.*

The Court is now presented with motions or letters from 119 putative defendants who seek to prevent disclosure of their identifying information or otherwise obtain dismissal from the lawsuit: thirty-three putative defendants have filed motions in which they generally deny using BitTorrent to download and distribute the plaintiff's movie,⁴ seventy-one putative defendants have

² Pursuant to Federal Rule of Civil Procedure 4(m), the plaintiff was required to name and serve defendants by September 21, 2010, which is the date within 120 days of filing its original Complaint. On September 24, 2010, the plaintiff requested additional time to name and serve the defendants because it had not received fully compliant responses from ISPs to the plaintiff's subpoenas. Pl.'s Mot. for Extension of Time to Name and Serve, Sept. 24, 2010, ECF No. 10. The Court granted the plaintiff a 180 day extension on September 28, 2010, which allowed the plaintiff to continue discovery until March 27, 2010. Minute Order, Sept. 28, 2010 (Urbina, J.). On April 4, 2010, the Court extended the plaintiff's time to name and serve putative defendants to June 13, 2011. ECF No. 120.

³ The Court's Order approving expedited discovery did not expressly order the plaintiff or ISPs to send notices to putative defendants before their identifying information was released in response to the plaintiff's subpoenas. Plaintiff's counsel, however, represented in a related case that a notice was attached to all subpoenas issued to ISPs for identifying information in cases where his law firm serves as plaintiff's counsel. Transcript of Mot. Hearing, at 50-51, *Wall of the Wild Movie, LLC. v. Smith*, No. 10-cv-455 (Mar. 1, 2011) ("Every single subpoena we sent to an ISP has the [notice approved by Judge Collyer in *Achte/Neunte Boll Kino Beteiligungs GMBH & Co, KG v. Does I-4,577*, No. 10-cv-00453 (D.D.C. July 22, 2010) (Minute Order approving Court-Directed Notice, ECF No. 36)] attached to it. And [ISP] Time Warner, I believe, reached an agreement on the form of that notice in Judge Collyer's court, and every single subpoena we sent since that date in every new case has that notice.").

⁴ See Janyth D. Girard, ECF No. 11 (IP address listed: 71.32.60146); Louis R. Carpenter, ECF No. 18 (IP address listed: 97.127.24.109); JoNeane Key, ECF No. 18 (No IP address listed); Sherry Porter, ECF No. 29 (No IP address listed); Michael B. Parker, ECF No. 31 (No IP address listed); James Kane, ECF No. 32 (No IP address listed); Jay R. Frydenlund, ECF No. 33 (IP address listed: 71.38.47.225); Debora L. Andrews, ECF No. 34 (IP address listed: 174.31.89.186); Jan H. Slater, ECF No. 35 (IP address listed: 71.212.5.157); Millwee Holler-Kanaga, ECF No. 36

filed motions to quash under on FED. R. CIV. P. 45(c)(3),⁵ seven putative defendants have filed

(IP address listed: 75.165.182.92); Ben Hatch, ECF No. 38 (No IP address listed); William C. Cook, Sr., ECF No. 41 (IP address listed: 71.217.225.229); Raghbir Singh, ECF No. 42 (No IP address listed); Arthur B. Cutting, ECF No. 44 (No IP address listed); LaMarr M. Jones, ECF No. 46 (No IP address listed); Richard DeHart, ECF No. 47 (IP address listed: 70.59.194.89); Byron Lee, ECF No. 48 (IP address listed: 96.40.190.149.00); Michael Koenig, ECF No. 54 (No IP address listed); Shey Davis, ECF No. 61 (No IP address listed); Judy Collins, ECF No. 69 (No IP address listed); Nick Hartmann, ECF No. 73 (No IP address listed); Khaled Hamed, ECF No. 103 (IP address listed: 68.184.152.100); Syed Mobeen, ECF No. 105 (No IP address listed); Chelsea Reitzner, ECF No. 106 (IP address listed: 24.183.109.103); Alan Stowers, ECF No. 107 (No IP address listed); Darryl Godfrey, ECF No. 109 (No IP address listed); Justin Solem, ECF No. 112 (No IP address listed); Aleksandr Baga, ECF No. 113 (IP address listed: 24.17.133.177); Adam Owensby, ECF No. 118 (No IP address listed); Chris Queen, ECF No. 138 (No IP address listed); Kaylin Werth, ECF No. 139 (IP address listed: 71.89.27.95); William White, ECF No. 141 (IP address listed: 66.190.77.95); Rita Shostak, ECF No. 149 (No IP address listed).

⁵ See Janyth D. Girard, ECF No. 11 (IP address listed: 71.32.60.146); Margaret Wenzek, ECF No. 15 (No IP address listed); Audrey Kalblinger, ECF No. 16 (No IP address listed); John Doe, ECF No. 18 (IP address listed: 67.40.214.85); John Doe, ECF No. 18 (IP address listed: 216.160.106.134); John Doe, ECF No. 18 (No IP address listed); Nicole G. Lipson, ECF No. 18 (No IP address listed); Kenneth G. Kupke, ECF No. 18 (No IP address listed); Delmar R. Towler, ECF No. 18 (No IP address listed); Richard L. Stellah, ECF No. 18 (No IP address listed); JoNeane Key, ECF No. 18 (No IP address listed); Darcie Dikeman, ECF No. 21 (No IP address listed); Jason Brittan, ECF No. 28 (No IP address listed); Sherry Porter, ECF No. 29 (No IP address listed); Michael B. Parker, ECF Nos. 31, 110 (No IP address listed); Jay R. Frydenlund, ECF No. 33 (IP address listed: 71.38.47.225); Debora L. Andrews, ECF No. 34 (IP address listed: 174.31.89.186); Millwee Holler-Kanaga, ECF No. 36 (IP address listed: 75.165.182.92); Ben Hatch, ECF No. 38 (No IP address listed); William C. Cook, Sr., ECF No. 41 (IP address listed: 71.217.225.229); A. Turner, ECF No. 45 (IP address listed: 216.161.89.109); Michael Koenig, ECF No. 54 (No IP address listed); Cheryl A. Lobo, ECF No. 56 (No IP address listed); Randall J. Azbill, Sr., ECF No. 57 (No IP address listed); John T. Krayner, ECF No. 58 (No IP address listed); Joseph M. Luria, ECF No. 59 (No IP address listed); Cameron J. Kennedy, ECF No. 60 (No IP address listed); David Allan Doll, ECF No. 62 (No IP address listed); Matthew Cohen, ECF No. 64 (IP address listed: 98.117.43.70); Joseph M. Orovic, ECF No. 65 (No IP address listed); Rowena K. Cruz, ECF No. 66 (No IP address listed); Miriam Adelson, ECF No. 67 (No IP address listed); Antonio R. Hinton, ECF No. 68 (No IP address listed); Judy Collins, ECF No. 69 (No IP address listed); Kenneth Kantorowicz, ECF No. 70 (IP address listed: 98.127.67.128); Jomy Joseph, ECF No. 74, (No IP address listed); Jonathan T. Payne, ECF No. 75 (No IP address listed); Carman I. Goodrich, ECF No. 76 (No IP address listed); John C. Jacobson, ECF No. 77 (No IP address listed); Ruth Shih, ECF No. 78 (No IP address listed); Sean E. Ringle, ECF No. 79 (No IP address listed); Simone J. Johnson, ECF No. 80 (No IP address listed); Jordan C. Neptune, ECF No. 81 (No IP address listed); Warren M. Gehl, ECF No. 82 (No IP address listed); Eric M. Miller, ECF No. 83 (No IP address listed); Richard T. Holbrook, II, ECF No. 84 (No IP address listed); Darren Choong Sik Hng, ECF No. 85 (No IP address listed); Todd D. Merrifield, ECF No. 86 (No IP address listed); Amelia Cardenas, ECF No. 95, (No IP address listed); Amanda J. Quast, ECF No. 96 (No IP address listed); Randy L. Morton, ECF No. 97 (No IP address listed); Nanci Lam, represented by Michael S. Lee, Esq, ECF No. 101 (No IP address listed); Samuel Neuenschwander, ECF No. 102 (IP address listed: 96.3.75.15); Khaled Hamed, ECF No. 103 (IP address listed: 68.184.152.100); Anita M. Dorrance, ECF No. 104 (No IP address listed); Aleksandr Baga, ECF No. 113 (IP address listed: 24.17.133.177); Adam Owensby, ECF No. 118 (No IP address listed); Erik E. Johnston, ECF No. 121 (No IP address listed); Leigh Norris, ECF No. 126 (No IP address listed); Michael Scott Davis, ECF No. 127 (No IP address listed); Matthew Alan O'Connell, ECF No. 128 (No IP address listed); Kathleen Gonzales, ECF No. 129 (No IP address listed); Neel N. Patel, ECF No. 130 (No IP address listed); Nancy Schwarz, ECF No. 131 (No IP address listed); Matthew J. Selck, ECF No. 132 (No IP address listed); Von R. Arnst, ECF No. 133 (No IP address listed); Aaron Tukey, ECF No. 136 (IP address listed: 68.116.170.119); Freightmen International, ECF No. 140 (No IP address listed); J. McCarthy, ECF No. 148 (IP address listed: 72.73.239.68); Rita Shostak, ECF No. 149 (No IP address listed).

motions to dismiss asserting that the putative defendants are improperly joined,⁶ and forty-two putative defendants have filed motions to dismiss based on lack of personal jurisdiction.⁷

Additionally, thirty-five putative defendants have filed motions for protective orders.⁸ For the reasons stated below, the Court denies all of these motions.

⁶ See John Doe, ECF No. 18 (No IP address listed); Nicole G. Lipson, ECF No. 18 (No IP address listed); Kenneth G. Kupke, ECF No. 18 (No IP address listed); Delmar R. Towler, ECF No. 18 (No IP address listed); Richard L. Stellah, ECF No. 18 (No IP address listed); Mary Jo Elgie, ECF No. 30 (IP address listed: 98.118.130.44); Aaron Tukey, ECF No. 136 (IP address listed: 68.116.170.119).

⁷ See John Doe, ECF No. 18 (No IP address listed); Nicole G. Lipson, ECF No. 18 (No IP address listed); Kenneth G. Kupke, ECF No. 18 (No IP address listed); Delmar R. Towler, ECF No. 18 (No IP address listed); Richard L. Stellah, ECF No. 18 (No IP address listed); Corbin Swan, ECF No. 43 (No IP address listed); Cheryl A. Lobo, ECF No. 56 (No IP address listed); Randall J. Azbill, Sr., ECF No. 57 (No IP address listed); John T. Krayner, ECF No. 58 (No IP address listed); Joseph M. Luria, ECF No. 59 (No IP address listed); Cameron J. Kennedy, ECF No. 60 (No IP address listed); David Allan Doll, ECF No. 62 (No IP address listed); Joseph M. Orovic, ECF No. 65 (No IP address listed); Rowena K. Cruz, ECF No. 66 (No IP address listed); Miriam Adelson, ECF No. 67 (No IP address listed); Antonio R. Hinton, ECF No. 68 (No IP address listed); Kenneth Kantorowicz, ECF No. 70 (IP address listed: 98.127.67.128); Jomy Joseph, ECF No. 74, (No IP address listed); Jonathan T. Payne, ECF No. 75 (No IP address listed); Carman I. Goodrich, ECF No. 76 (No IP address listed); John C. Jacobson, ECF No. 77 (No IP address listed); Ruth Shih, ECF No. 78 (No IP address listed); Sean E. Ringle, ECF No. 79 (No IP address listed); Simone J. Johnson, ECF No. 80 (No IP address listed); Jordan C. Neptune, ECF No. 81 (No IP address listed); Warren M. Gehl, ECF No. 82 (No IP address listed); Eric M. Miller, ECF No. 83 (No IP address listed); Richard T. Holbrook, II, ECF No. 84 (No IP address listed); Darren Choong Sik Hng, ECF No. 85 (No IP address listed); Todd D. Merrifield, ECF No. 86 (No IP address listed); Amelia Cardenas, ECF No. 95, (No IP address listed); Amanda J. Quast, ECF No. 96 (No IP address listed); Randy L. Morton, ECF No. 97 (No IP address listed); Samuel Neuenschwander, ECF No. 102 (IP address listed: 96.3.75.15); Jeff Scherer, ECF No. 111 (IP address listed: 184.96.91.86); Erik E. Johnston, ECF No. 121 (No IP address listed); Leigh Norris, ECF No. 126 (No IP address listed); Michael Scott Davis, ECF No. 127 (No IP address listed); Neel N. Patel, ECF No. 130 (No IP address listed); Matthew J. Selck, ECF No. 132 (No IP address listed); Aaron Tukey, ECF No. 136 (IP address listed: 68.116.170.119); J. McCarthy, ECF No. 148 (IP address listed: 72.73.239.68).

⁸ See John Doe, ECF No. 18 (No IP address listed); Nicole G. Lipson, ECF No. 18 (No IP address listed); Kenneth G. Kupke, ECF No. 18 (No IP address listed); Delmar R. Towler, ECF No. 18 (No IP address listed); Richard L. Stellah, ECF No. 18 (No IP address listed); Cheryl A. Lobo, ECF No. 56 (No IP address listed); Randall J. Azbill, Sr., ECF No. 57 (No IP address listed); John T. Krayner, ECF No. 58 (No IP address listed); Joseph M. Luria, ECF No. 59 (No IP address listed); Cameron J. Kennedy, ECF No. 60 (No IP address listed); David Allan Doll, ECF No. 62 (No IP address listed); Joseph M. Orovic, ECF No. 65 (No IP address listed); Miriam Adelson, ECF No. 67 (No IP address listed); Antonio R. Hinton, ECF No. 68 (No IP address listed); Jomy Joseph, ECF No. 74, (No IP address listed); Jonathan T. Payne, ECF No. 75 (No IP address listed); Carman I. Goodrich, ECF No. 76 (No IP address listed); John C. Jacobson, ECF No. 77 (No IP address listed); Ruth Shih, ECF No. 78 (No IP address listed); Sean E. Ringle, ECF No. 79 (No IP address listed); Simone J. Johnson, ECF No. 80 (No IP address listed); Jordan C. Neptune, ECF No. 81 (No IP address listed); Warren M. Gehl, ECF No. 82 (No IP address listed); Eric M. Miller, ECF No. 83 (No IP address listed); Richard T. Holbrook, II, ECF No. 84 (No IP address listed); Darren Choong Sik Hng, ECF No. 85 (No IP address listed); Todd D. Merrifield, ECF No. 86 (No IP address listed); Amelia Cardenas, ECF No. 95, (No IP address listed); Amanda J. Quast, ECF No. 96 (No IP address listed); Randy L. Morton, ECF No. 97 (No IP address listed); Erik E. Johnston, ECF No. 121 (No IP address listed); Kathleen Gonzales, ECF No. 129 (No IP address listed); Neel N. Patel, ECF No. 130 (No IP address listed); Matthew J. Selck, ECF No. 132 (No IP address listed); J. McCarthy, ECF No. 148 (IP address listed: 72.73.239.68).

II. MOTIONS TO QUASH UNDER FEDERAL RULE OF CIVIL PROCEDURE 45

Seventy-one putative defendants have filed motions to quash the plaintiff's subpoenas issued to ISPs for the putative defendants' identifying information. These motions assert three arguments: First, the putative defendant filing the motion did not engage in the alleged illegal conduct and the plaintiff should therefore be prevented from obtaining the putative defendant's identifying information. Second, the subpoena should be quashed because it "requires disclosure of privileged or other protected matter" under FED. R. CIV. P. 45(c)(3)(A)(iii). Third, the plaintiff's subpoenas subject the putative defendant filing the motion to an undue burden under FED. R. CIV. P. 45(c)(3)(A)(iv). All of these arguments are unavailing.

Under Federal Rule of Civil Procedure 45(c), the Court must quash a subpoena when, *inter alia*, it "requires disclosure of privileged or other protected matter, if no exception or waiver applies" or "subjects a person to undue burden." FED. R. CIV. P. 45(c)(3)(A)(iii)-(iv). A general denial of engaging in copyright infringement is not a basis for quashing the plaintiff's subpoena. It may be true that the putative defendants who filed motions and letters denying that they engaged in the alleged conduct did not illegally infringe the plaintiff's copyrighted movie, and the plaintiff may, based on its evaluation of their assertions, decide not to name these individuals as parties in this lawsuit. On the other hand, the plaintiff may decide to name them as defendants in order to have an opportunity to contest the merits and veracity of their defenses in this case. In other words, if these putative defendants are named as defendants in this case, they may deny allegations that they used BitTorrent to download and distribute illegally the plaintiff's movie, present evidence to corroborate that defense, and move to dismiss the claims against them. A general denial of liability, however, is not a basis for quashing the plaintiff's subpoenas and preventing the plaintiff from obtaining the putative defendants' identifying information. That would deny the plaintiff access to the information critical to bringing these individuals properly

into the lawsuit to address the merits of both the plaintiff's claim and their defenses. *See Achte/Neunte Boll Kino Beteiligungs GMBH & Co, KG v. Does 1-4*, 577, 736 F. Supp. 2d 212, 215 (D.D.C. 2010) (denying motions to quash filed by putative defendants in BitTorrent file-sharing case and stating that putative defendants' "denial of liability may have merit, [but] the merits of this case are not relevant to the issue of whether the subpoena is valid and enforceable. In other words, they may have valid defenses to this suit, but such defenses are not at issue [before the putative defendants are named parties]."); *see also Fonovisa, Inc. v. Does 1-9*, No. 07-1515, 2008 WL 919701, at *8 (W.D. Pa. Apr. 3, 2008) (if a putative defendant "believes that it has been improperly identified by the ISP, [the putative defendant] may raise, at the appropriate time, any and all defenses, and may seek discovery in support of its defenses.").

Thirty putative defendants urge the Court to quash the plaintiff's subpoenas based upon their privacy interests.⁹ Rule 45(c)(3)(A)(iii) instructs a Court to quash a subpoena if it "requires disclosure of privileged or other protected matter." FED. R. CIV. P. 45(c)(3)(A)(iii). This rule, however, does not apply here. The Court recognizes that the putative defendants' First Amendment right to anonymous speech is implicated by disclosure of their identifying information. *See Sony Music Entm't, Inc. v. Does 1-40*, 326 F. Supp. 2d 556, 564 (S.D.N.Y.

⁹ *See* Louis R. Carpenter, ECF No. 18 (IP address listed: 97.127.24.109); James Kane, ECF No. 32 (No IP address listed); Jan H. Slater, ECF No. 35 (IP address listed: 71.21.25.157); Sara Sherwood, ECF No. 37 (IP address listed: 00:13:10:b9:71:a5); Sandra Dockery, ECF No. 39 (No IP address listed); Colin Quennell, ECF No. 40 (No IP address listed); Richard DeHart, ECF No. 47 (IP address listed: 70.59.194.89); Byron Lee, ECF No. 48 (IP address listed: 96.40.190.149.00); Adam Delgado, ECF No. 49 (No IP address listed); Karen Eiriz, ECF No. 50 (No IP address listed); Lucy A. Marsh, ECF No. 53 (No IP address listed); Jonathan D. Coleman, ECF No. 63 (No IP address listed); Aran Bedarian, ECF No. 71 (No IP address listed); Morris Carrejo, ECF No. 99 (No IP address listed); Charles Ellsworth, ECF No. 100 (No IP address listed); Anita M. Dorrance, ECF No. 104 (No IP address listed); Syed Mobeen, ECF No. 105 (No IP address listed); Chelsea Reitzner, ECF No. 106 (IP address listed: 24.183.109.103); Alan Stowers, ECF No. 107 (No IP address listed); Shani Myers, ECF No. 108 (No IP address listed); Darryl Godfrey, ECF No. 109 (No IP address listed); Justin Solem, ECF No. 112 (No IP address listed); Kathryn Lanier, ECF No. 119 (No IP address listed); Mary Woods, ECF No. 135 (IP address listed: 75.137.118.90); Guntars Rizijs, ECF No. 137 (No IP address listed); Chris Queen, ECF No. 138 (No IP address listed); Kaylin Werth, ECF No. 139 (IP address listed: 71.89.27.95); William White, ECF No. 141 (IP address listed: 66.190.77.95); Rita Shostak, ECF No. 149 (No IP address listed).

2004) (“the file sharer may be expressing himself or herself through the music selected and made available to others.”); *see also London-Sire Records, Inc. v. Doe I*, 542 F. Supp. 2d 153, 163 (D. Mass. 2008). Nevertheless, whatever asserted First Amendment right to anonymity the putative defendants may have in this context does not shield them from allegations of copyright infringement.¹⁰ *See Arista Records LLC v. Does I-19*, 551 F. Supp. 2d 1, 8 (D.D.C. 2008) (“First Amendment privacy interests are exceedingly small where the ‘speech’ is the alleged infringement of copyrights.”); *Achte/Neunte*, 736 F. Supp. 2d at 216 n.2 (“the protection afforded to such speech is limited and gives way in the face of a prima facie showing of copyright infringement”); *West Bay One, Inc. v. Does I-1653*, 270 F.R.D. 13, 16 n.4 (D.D.C. 2010) (same); *Sony*, 326 F. Supp. 2d at 567 (First Amendment right of alleged file-sharers to remain anonymous “must give way to the plaintiffs’ right to use the judicial process to pursue what appear to be meritorious copyright infringement claims.”); *Elektra Entm’t Grp., Inc. v. Does I-9*, No. 04-2289, 2004 WL 2095581, at *4-5 (S.D.N.Y. Sept. 8, 2004) (finding that First Amendment right to anonymity is overridden by plaintiff’s right to protect copyright).

Finally, the argument that the plaintiff’s subpoenas subject putative defendants to an undue burden is also unavailing. Putative defendants essentially argue that the plaintiff’s subpoenas require them to litigate in a forum in which they should not be subject to personal jurisdiction, which causes them hardship. As explained more fully *infra*, the putative defendants’ personal jurisdiction arguments are premature at this time because they have not been named as parties to this lawsuit. Given that they are not named parties, the putative defendants are not required to respond to the allegations presented in the plaintiff’s Complaint or

¹⁰ A more expansive discussion of the putative defendants’ First Amendment rights in this case is contained in the Court’s Memorandum Opinion filed March 22, 2011 in a similar case involving putative defendants accused of using the BitTorrent file-sharing technology to download and distribute illegally copyright works. *See Call of the Wild Movie, LLC v. Does I-1,062*, No. 10-cv-455, 2011 WL 996786 at *10-15 (D.D.C. Mar. 22, 2011).

otherwise litigate in this district. The plaintiff has issued subpoenas to the putative defendants' ISPs, not to the putative defendants themselves. Consequently, the putative defendants face no obligation to produce any information under the subpoenas issued to their respective ISPs and cannot claim any hardship, let alone undue hardship.¹¹

The plaintiff's subpoenas requesting the putative defendants' identifying information do not subject the putative defendants to an undue burden nor is the plaintiff's request for the information outweighed by any privacy interest or First Amendment right to anonymity. Moreover, a general denial of liability is not a proper basis to quash the plaintiff's subpoenas. Accordingly, the putative defendants' motions, under Federal Rule of Civil Procedure 45(c)(3), to quash the subpoenas are denied.

III. MOTIONS FOR PROTECTIVE ORDERS

Thirty-five putative defendants have filed motions for protective orders seeking to protect their identities from being disclosed to the plaintiff.¹² Rule 26(c) provides that a court may "issue

¹¹ Any reliance the putative defendants may have placed on Federal Rule of Civil Procedure 45(c)(3)(A)(ii) as an alternate basis for quashing the plaintiff's subpoenas is therefore also misplaced. Rule 45(c)(3)(A)(ii) requires the Court to quash a subpoena when the subpoena "requires a person who is neither a party nor a party's officer to travel more than 100 miles from where that person resides, is employed, or regularly transacts business in person" The putative defendants are not required to respond to the plaintiff's subpoenas or otherwise travel away from their homes or places of employment.

¹² See John Doe, ECF No. 18 (No IP address listed); Nicole G. Lipson, ECF No. 18 (No IP address listed); Kenneth G. Kupke, ECF No. 18 (No IP address listed); Delmar R. Towler, ECF No. 18 (No IP address listed); Richard L. Stellah, ECF No. 18 (No IP address listed); Cheryl A. Lobo, ECF No. 56 (No IP address listed); Randall J. Azbill, Sr., ECF No. 57 (No IP address listed); John T. Krayner, ECF No. 58 (No IP address listed); Joseph M. Luria, ECF No. 59 (No IP address listed); Cameron J. Kennedy, ECF No. 60 (No IP address listed); David Allan Doll, ECF No. 62 (No IP address listed); Joseph M. Orovic, ECF No. 65 (No IP address listed); Miriam Adelson, ECF No. 67 (No IP address listed); Antonio R. Hinton, ECF No. 68 (No IP address listed); Jomy Joseph, ECF No. 74, (No IP address listed); Jonathan T. Payne, ECF No. 75 (No IP address listed); Carman I. Goodrich, ECF No. 76 (No IP address listed); John C. Jacobson, ECF No. 77 (No IP address listed); Ruth Shih, ECF No. 78 (No IP address listed); Sean E. Ringle, ECF No. 79 (No IP address listed); Simone J. Johnson, ECF No. 80 (No IP address listed); Jordan C. Neptune, ECF No. 81 (No IP address listed); Warren M. Gehl, ECF No. 82 (No IP address listed); Eric M. Miller, ECF No. 83 (No IP address listed); Richard T. Holbrook, II, ECF No. 84 (No IP address listed); Darren Choong Sik Hng, ECF No. 85 (No IP address listed); Todd D. Merrifield, ECF No. 86 (No IP address listed); Amelia Cardenas, ECF No. 95, (No IP address listed); Amanda J. Quast, ECF No. 96 (No IP address listed); Randy L. Morton, ECF No. 97 (No IP address listed); Erik E. Johnston, ECF No. 121 (No IP address listed); Kathleen Gonzales, ECF No. 129 (No IP address listed); Neel N. Patel, ECF No. 130 (No IP address listed); Matthew J. Selck, ECF No. 132 (No

an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense.” FED. R. CIV. P. 26(c)(1).¹³ Such protective orders may forbid disclosure altogether, or, among other measures, “limit[] the scope of disclosure or discovery to certain matters.” FED. R. CIV. P. 26(c)(1)(A) and (D). “[A]lthough Rule 26(c) contains no specific reference to privacy or to other rights or interests that may be implicated, such matters are implicit in the broad purpose and language of the Rule.” *In re Sealed Case (Medical Records)*, 381 F.3d 1205, 1215 (D.C. Cir. 2004) (quoting *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 35 n.21 (1984)).

As elaborated above, the putative defendants are not subject to the plaintiff’s subpoenas, and therefore do not face any “annoyance, embarrassment, oppression, or undue burden or expense” from the plaintiff’s discovery request. *See* FED. R. CIV. P. 26(c)(1). To the extent that the putative defendants seek protective orders to prevent disclosure of private identifying information, the Court has held that the putative defendants’ First Amendment rights to anonymity in the context of their BitTorrent activity is minimal and outweighed by the plaintiff’s need for the putative defendants’ identifying information in order to protect its copyrights. *See Call of the Wild Movie, LLC v. Does 1-1,062*, No. 10-cv-455, 2011 WL 996786 at *10-15 (D.D.C. Mar. 22, 2011). The putative defendants’ requests for protective orders are therefore denied.

IV. MOTIONS TO DISMISS BASED ON IMPROPER JOINDER

IP address listed); J. McCarthy, ECF No. 148 (IP address listed: 72.73.239.68). The Court directed the Clerk to file these motions under seal pending resolution of their motions for protective orders. The Court denies these motions in the instant Memorandum Opinion, and, as reflected in the Order accompanying this Memorandum Opinion, the Clerk is directed to unseal the ECF docket entries: 56-60, 62, 64-68, 73-86, 94-98, 108, 119, 121, 129, 130-134, and 148.

¹³ Many of the putative defendants state that they seek protective orders pursuant to Federal Rule of Civil Procedure 37. The Court assumes, however, that they seek protective orders under Federal Rule of Civil Procedure 26(c), and construes their motions accordingly.

Seven putative defendants argue that they should be dismissed from the lawsuit because the plaintiff has improperly joined them with other putative defendants.¹⁴ The putative defendants' argument that they are improperly joined may be meritorious should they be named as defendants in this action. At this stage in the litigation, however, when discovery is underway to learn identifying facts necessary to permit service on Doe defendants, joinder, under Federal Rule of Civil Procedure 20(a)(2), of unknown parties identified only by IP addresses is proper. As discussed below, this conclusion is further supported by the allegations set forth in the Complaint, which sufficiently establishes a *prima facie* case of infringement of plaintiff's copyright by users of the same file-sharing software program that operates through simultaneous and sequential computer connections and data transfers among the users.

At the outset, the Court notes that the remedy for improper joinder under Federal Rule of Civil Procedure 21 is not dismissal of the action.¹⁵ FED. R. CIV. P. 21 ("Misjoinder of parties is not a ground for dismissing an action."). Improper joinder may be remedied by "drop[ping]" a party and severing claims against that party. FED. R. CIV. P. 21 ("On motion or on its own, the Court may at any time, on just terms, add or drop a party."). This would simply create separate actions containing the same claims against the same putative defendants. *See Bailey v. Fulwood*,

¹⁴ See John Doe, ECF No. 18 (No IP address listed); Nicole G. Lipson, ECF No. 18 (No IP address listed); Kenneth G. Kupke, ECF No. 18 (No IP address listed); Delmar R. Towler, ECF No. 18 (No IP address listed); Richard L. Stellah, ECF No. 18 (No IP address listed); Mary Jo Elgie, ECF No. 30 (IP address listed: 98.118.130.44); Aaron Tukey, ECF No. 136 (IP address listed: 68.116.170.119).

¹⁵ Rule 21 does not set forth what constitutes misjoinder, but "it is well-settled that parties are misjoined when the preconditions of permissive joinder set forth in Rule 20(a) have not been satisfied." *Disparte v. Corporate Exec. Bd.*, 223 F.R.D. 7, 12 (D.D.C. 2004) (citation omitted). Courts have also read Rule 21 in conjunction with Rule 42(b), which allows the court to sever claims in order to avoid prejudice to any party. *M.K. v. Tenet*, 216 F.R.D. 133, 138 (D.D.C. 2002); see also FED. R. CIV. P. 42(b) ("For convenience, to avoid prejudice, or to expedite and economize, the court may order a separate trial of one or more separate issues, claims, crossclaims, counterclaims, or third-party claims."). In addition to the two requirements of Rule 20(a)(2), courts therefore also consider whether joinder would prejudice any party or result in needless delay. *See Lane v. Tschetter*, No. 05-1414, 2007 WL 2007493, at *7 (D.D.C. July 10, 2007); *Tenet*, 216 F.R.D. at 138.

No. 10-463, 2010 U.S. Dist. LEXIS 141356, at *11 (D.D.C. Feb. 15, 2010); *In re Brand-Name Prescription Drugs Antitrust Litig.*, 264 F. Supp. 2d 1372, 1376 (J.P.M.L. 2003) (“[S]everance of claims under Rule 21 results in the creation of separate actions.”). The Court may exercise discretion regarding the proper time to sever parties, and this determination includes consideration of judicial economy and efficiency. *See Disparte v. Corporate Exec. Bd.*, 223 F.R.D. 7, 10 (D.D.C. 2004) (Permissive joinder under Federal Rule 20 is designed “to promote trial convenience and expedite the resolution of lawsuits,” quoting *Puricelli v. CNA Ins. Co.*, 185 F.R.D. 139, 142 (N.D.N.Y. 1999)). For example, in *London-Sire Records, Inc. v. Doe 1*, 542 F. Supp. 2d 153 (D. Mass. 2008), the court consolidated separate Doe lawsuits for copyright infringement since the “cases involve[d] similar, even virtually identical, issues of law and fact: the alleged use of peer-to-peer software to share copyrighted sound recordings and the discovery of defendants’ identities through the use of a Rule 45 subpoena to their internet service provider.” *Id.* at 161. In the court’s view, consolidation of the separate lawsuits for purposes of expedited discovery “ensures administrative efficiency for the Court, the plaintiffs, and the ISP, and allows the defendants to see the defenses, if any, that other John Does have raised.” *Id.* The court noted that, after discovery, “[t]he case against each Doe [would] be individually considered for purposes of any rulings on the merits,” and the putative defendants could “renew the severance request before trial if the case proceeds to that stage.” *Id.* at 161 n.7.

In addition to providing efficiencies for expedited discovery on jurisdictional issues, defendants may be properly joined in one action when claims arise from the same transaction or occurrence or series of transactions or occurrences; and any question of law or fact in the action is common to all defendants. FED. R. CIV. P. 20(a)(2); *see also Montgomery v. STG Int’l, Inc.*, 532 F. Supp. 2d 29, 35 (D.D.C. 2008) (interpreting Rule 20(a)(1), which has the same

requirements as Rule 20(a)(2)). The requirements for permissive joinder are “liberally construed in the interest of convenience and judicial economy in a manner that will secure the just, speedy, and inexpensive determination of the action.” *Lane v. Tschetter*, No. 05-1414, 2007 WL 2007493, at *7 (D.D.C. July 10, 2007) (internal quotation omitted); *see also Davidson v. District of Columbia*, 736 F. Supp. 2d 115, 119 (D.D.C. 2010). Thus, “the impulse is toward entertaining the broadest possible scope of action consistent with fairness to the parties; [and] joinder of claims, parties, and remedies is strongly encouraged.” *United Mine Workers of Am. v. Gibbs*, 383 U.S. 715, 724 (1966).

In the present case, the plaintiff has met all the requirements for permissive joinder under Federal Rule of Civil Procedure 20(a)(2). The first requirement is that claims must “aris[e] out of the same transaction, occurrence, or series of transactions or occurrences.” FED. R. CIV. P. 20(a)(2)(A). This essentially requires claims asserted against joined parties to be “logically related.” *Disparte*, 223 F.R.D. at 10. This is a flexible test and courts seek the “broadest possible scope of action.” *Lane*, 2007 WL 2007493, at *7 (quoting *Gibbs*, 383 U.S. at 724).

The plaintiff alleges that the putative defendants used the BitTorrent file-sharing protocol to distribute illegally the plaintiff’s motion picture. Compl., ¶ 3. This file-sharing protocol “makes every downloader also an uploader of the illegally transferred file(s). This means that every . . . user who has a copy of the infringing copyrighted material on a torrent network must necessarily also be a source of download for that infringing file.” *Id.* The plaintiff further asserts that the “nature of a BitTorrent protocol [is that] any seed peer that has downloaded a file prior to the time a subsequent peer downloads the same file is automatically a source for the subsequent peer so long as that first seed peer is online at the time the subsequent peer downloads a file.” *Id.* at ¶ 4.

Based on these allegations, the plaintiff's claims against the putative defendants are logically related at this stage in the litigation. According to the plaintiff, each putative defendant is a possible source for the plaintiff's motion picture, and may be responsible for distributing this copyrighted work to the other putative defendants, who are also using the same file-sharing protocol to copy and distribute the same copyrighted work. *See Disparte*, 223 F.R.D. at 10 (to satisfy Rule 20(a)(2)(A) claims must be "logically related" and this test is "flexible."). While the putative defendants may be able to rebut these allegations at a later date, at this procedural juncture the plaintiff has sufficiently alleged that its claims against the putative defendants potentially stem from the same transaction or occurrence, and are logically related. *See Arista Records LLC v. Does I-19*, 551 F. Supp. 2d 1, 11 (D.D.C. 2008) ("While the Courts notes that the remedy for improper joinder is severance and not dismissal, the Court also finds that this inquiry is premature without first knowing Defendants' identities and the actual facts and circumstances associated with Defendants' conduct." (internal citation omitted)).

Some courts in other jurisdictions have granted motions by putative defendants for severance in analogous copyright infringement cases against unknown users of peer-to-peer file-sharing programs for failure to meet the "same transaction or occurrence test" in Rule 20(a)(2). Those courts have been confronted with bare allegations that putative defendants used the same peer-to-peer network to infringe copyrighted works and found those allegations were insufficient for joinder. *See, e.g., IO Grp., Inc. v. Does I-19*, No. 10-03851, 2010 WL 5071605, at *8-12 (N.D. Cal. Dec. 7, 2010); *Arista Records, LLC v. Does I-11*, No. 07-cv-2828, 2008 WL 4823160, at *6 (N.D. Ohio Nov. 3, 2008) ("merely alleging that the Doe Defendants all used the same ISP and file-sharing network to conduct copyright infringement without asserting that they acted in concert was not enough to satisfy the same series of transactions requirement under the

Federal Rules.”); *LaFace Records, LLC v. Does 1-38*, No. 5:07-cv-298, 2008 WL 544992, at *3 (E.D. N.C. Feb. 27, 2008) (severing putative defendants in file-sharing case not involving BitTorrent technology, noting that “other courts have commonly held that where there is no assertion that multiple defendants have acted in concert, joinder is improper.”); *Interscope Records v. Does 1-25*, No. 6:04-cv-197, 2004 U.S. Dist. LEXIS 27782 (M.D. Fla. Apr. 1, 2004) (adopting Mag. J. Report and Recommendation at *Interscope Records v. Does 1-25*, No. 6:04-cv-197, 2004 U.S. Dist. LEXIS 27782 (M.D. Fla. Apr. 1, 2004)). That is not the case here.

The plaintiff has provided detailed allegations about how the BitTorrent technology differs from other peer-to-peer file-sharing programs and necessarily engages many users simultaneously or sequentially to operate. *See Columbia Pictures Indus. v. Fung*, No. 06-5578, 2009 U.S. Dist. LEXIS 122661, at *7 (C.D. Cal. Dec. 21, 2009) (BitTorrent “is unique from that of previous [P2P] systems such as Napster and Grokster. Rather than downloading a file from an individual user, [BitTorrent users download] from a number of host computers that possess the file simultaneously. . . . The BitTorrent client application [] simultaneously downloads the pieces of the content file from as many users as are available at the time of the request, and then reassembles the content file on the requesting computer when the download is complete. Once a user downloads a given content file, he also becomes a source for future requests and downloads.”). Specifically, BitTorrent creates a “swarm” in which “each additional user becomes a part of the network from where the file can be downloaded . . . [U]nlike a traditional peer-to-peer network, each new file downloader is receiving a different piece of the data from each user who has already downloaded the file that together comprises the whole.” Compl., ¶ 3.

At least one court has not been persuaded that allegations of copyright infringement by users of BitTorrent satisfy the requirement of Rule 20. *See, e.g., Lightspeed v. Does 1-1000*, No.

10-cv-5604, 2011 U.S. Dist. LEXIS 35392, at *4-7 (N.D. Ill. Mar. 31, 2011) (finding that Doe defendants using BitTorrent technology were misjoined on the basis that the putative defendants were not involved in the “same transaction, occurrence, or series of transactions or occurrence” under FED. R. CIV. P. 20(a)(2)(A)); *Millennium TGA Inc. v. Does 1-800*, No. 10-cv-5603, 2011 U.S. Dist. LEXIS 35406, at *3-5 (N.D. Ill. Mar. 31, 2011) (same). In those cases, the court did not discuss the precise nature of the BitTorrent technology, which enables users to contribute to each other’s infringing activity of the same work as part of a “swarm.” In any event, by contrast to the instant claim of infringement of a single copyrighted work by the putative defendants, the plaintiffs in *Lightspeed* and *Millennium TGA Inc.* alleged infringement of multiple works, a factor that may undermine the requisite showing of concerted activity to support joinder.

The second requirement for proper joinder under Rule 20(a)(2) is that the plaintiff’s claims against the putative defendants must contain a common question of law or fact. FED. R. CIV. P. 20(a)(2)(B); *see also Disparte*, 223 F.R.D. at 11. The plaintiff has met this requirement as well. The plaintiff must establish against each putative defendant the same legal claims concerning the validity of the copyright at issue and the infringement of the exclusive rights reserved to the plaintiff as the copyright holder. Furthermore, the putative defendants are alleged to have utilized the same BitTorrent file-sharing protocol to distribute and download illegally the plaintiff’s movie and, consequently, factual issues related to how BitTorrent works and the methods used by the plaintiff to investigate, uncover and collect evidence about the infringing activity will be essentially identical for each putative defendant. *See* Compl., ¶ 3. The Court recognizes that each putative defendant may later present different factual and substantive legal defenses, but that does not defeat, at this stage of the proceedings, the commonality in facts and legal claims that support joinder under Rule 20(a)(2)(B).

In addition to the two requirements for permissive joinder under Rule 20(a)(2), the Court must also assess whether joinder would prejudice the parties or result in needless delay. *See Lane*, 2007 WL 2007493, at *7; *M.K. v. Tenet*, 216 F.R.D. 133, 138 (D.D.C. 2002). At this stage in the litigation, it will not. The putative defendants are currently identified only by their IP addresses and are not named parties. They are thus not required to respond to the plaintiff's allegations or assert a defense. The putative defendants may be able to demonstrate prejudice should the plaintiff name and proceed with a case against them, but they cannot demonstrate any harm that is occurring to them before that time. In addition, rather than result in needless delay, joinder of the putative defendants facilitates jurisdictional discovery and expedites the process of obtaining identifying information, which is prerequisite to reaching the merits of the plaintiff's claims. The Court therefore concludes that at this procedural juncture, the plaintiff has met the requirements of permissive joinder under Rule 20(a)(2) and joinder of the putative defendants is proper.¹⁶

The Court reaches this conclusion cognizant of the significant burdens on the court and judicial economy posed by the sheer number of putative defendants that the plaintiff seeks to join in a single lawsuit. These concerns are legitimately shared by other courts across the country that are confronting copyright infringement cases involving allegations of illegal file-sharing of copyrighted works by unprecedented numbers of Doe defendants, and the multitude of motions from interested parties that such suits engender. *Lightspeed*, 2011 U.S. Dist. LEXIS 35392, at *7 (“given the number of ‘potential’ defendants (i.e., Does 1-1000), [the] court could be faced with hundreds of factually unique motions to dismiss, quash or sever from potential defendants

¹⁶ For a more expansive discussion regarding the propriety of joining the putative defendants in this case, see the Court's Memorandum Opinion filed March 22, 2011 in a similar case involving putative defendants accused of using the BitTorrent file-sharing technology to download and distribute illegally copyright works. *Call of the Wild Movie, LLC v. Does 1-1,062*, No. 10-cv-455, 2011 WL 996786 at *4-7 (D.D.C. Mar. 22, 2011).

located all over the country.”); *Millennium TGA Inc.*, 2011 U.S. Dist. LEXIS 35406, at *5 (same). Courts have varying thresholds for the exercise of their discretion to sever defendants in such cases. *See Bridgeport Music, Inc. v. IIC Music*, 202 F.R.D. 229, 232-33 (M.D. Tenn. 2001) (even if joinder of over 700 named defendants was proper because claims arose from the same series of occurrences, “the Court would exercise the discretion afforded it to order a severance to avoid causing unreasonable prejudice and expense to Defendants and to avoid a great inconvenience to the administration of justice”).

This Court similarly must evaluate judicial economy and the administrative burdens of managing such cases, set against the challenge broad-scale allegedly infringing activity represents for the copyright owners. Copyright owners’ efforts to protect their copyrighted works through Doe actions are “costly[,] time consuming[,] . . . cumbersome and expensive.” *In re Charter Commc’ns, Inc., Subpoena Enforcement Matter*, 393 F.3d 771, 782 (8th Cir. 2005) (Murphy, J., dissenting). Yet, copyright owners have limited alternatives to obtain redress for infringement of their protected works other than such lawsuits. *See Arista Records LLC v. Does 1-27*, 584 F. Supp. 2d 240, 252 (D. Me. 2008) (“the Court begins with the premise that the Plaintiffs have a statutorily protected interest in their copyrighted material and that the Doe Defendants, at least by allegation, have deliberately infringed that interest without consent or payment. Under the law, the Plaintiffs are entitled to protect their copyrighted material and it is difficult to discern how else in this unique circumstance the Plaintiffs could act. Not to act would be to allow those who would take what is not theirs to remain hidden behind their ISPs and to diminish and even destroy the intrinsic value of the Plaintiffs’ legal interests.”); *In re Charter Commc’ns, Inc.*, 393 F.3d at 775 n.3 (“[A]s a practical matter, copyright owners cannot deter unlawful peer-to-peer file transfers unless they can learn the identities of persons engaged in that

activity.”). Courts must nonetheless maintain supervision of these lawsuits and, at some point, the sheer number of putative defendants involved in a single case may necessitate severance.

Joinder in this case at this stage of the litigation is proper. Should the putative defendants be named in the Complaint, they may raise the argument that they are improperly joined, under Federal Rule of Civil Procedure 20, and move to sever, under Federal Rule of Civil Procedure 21. Severance prior to that point, as numerous other courts both in and outside this District have held, is premature. *See, e.g., Achte/Neunte Boll Kino Beteiligungs GMBH & Co, KG v. Does I-4,577*, No. 10-cv-00453, ECF No. 34 (D.D.C. July 2, 2010) (Collyer, J.); *West Bay One, Inc. v. Does I-1653*, No. 10-cv-00481, ECF No. 25 (D.D.C. July 2, 2010) (Collyer, J.); *Arista Records LLC v. Does I-19*, 551 F. Supp. 2d 1, 11 (D.D.C. 2008) (Kollar-Kotelly, J.); *London-Sire Records, Inc. v. Doe I*, 542 F. Supp. 2d 153, 161 n.7 (D. Mass. 2008); *Sony Music Entm’t, Inc. v. Does I-40*, 326 F. Supp. 2d 556, 568 (S.D.N.Y. 2004).

V. MOTIONS TO DISMISS BASED ON LACK OF PERSONAL JURISDICTION

Forty-two putative defendants argue that they should be dismissed from the lawsuit because the Court lacks personal jurisdiction over them.¹⁷ To support this argument, they supply

¹⁷ *See* John Doe, ECF No. 18 (No IP address listed); Nicole G. Lipson, ECF No. 18 (No IP address listed); Kenneth G. Kupke, ECF No. 18 (No IP address listed); Delmar R. Towler, ECF No. 18 (No IP address listed); Richard L. Stellah, ECF No. 18 (No IP address listed); Corbin Swan, ECF No. 43 (No IP address listed); Cheryl A. Lobo, ECF No. 56 (No IP address listed); Randall J. Azbill, Sr., ECF No. 57 (No IP address listed); John T. Krayner, ECF No. 58 (No IP address listed); Joseph M. Luria, ECF No. 59 (No IP address listed); Cameron J. Kennedy, ECF No. 60 (No IP address listed); David Allan Doll, ECF No. 62 (No IP address listed); Joseph M. Orovic, ECF No. 65 (No IP address listed); Rowena K. Cruz, ECF No. 66 (No IP address listed); Miriam Adelson, ECF No. 67 (No IP address listed); Antonio R. Hinton, ECF No. 68 (No IP address listed); Kenneth Kantorowicz, ECF No. 70 (IP address listed: 98.127.67.128); Jomy Joseph, ECF No. 74, (No IP address listed); Jonathan T. Payne, ECF No. 75 (No IP address listed); Carman I. Goodrich, ECF No. 76 (No IP address listed); John C. Jacobson, ECF No. 77 (No IP address listed); Ruth Shih, ECF No. 78 (No IP address listed); Sean E. Ringle, ECF No. 79 (No IP address listed); Simone J. Johnson, ECF No. 80 (No IP address listed); Jordan C. Neptune, ECF No. 81 (No IP address listed); Warren M. Gehl, ECF No. 82 (No IP address listed); Eric M. Miller, ECF No. 83 (No IP address listed); Richard T. Holbrook, II, ECF No. 84 (No IP address listed); Darren Choong Sik Hng, ECF No. 85 (No IP address listed); Todd D. Merrifield, ECF No. 86 (No IP address listed); Amelia Cardenas, ECF No. 95, (No IP address listed); Amanda J. Quast, ECF No. 96 (No IP address listed); Randy L. Morton, ECF No. 97 (No IP address listed); Samuel Neuenschwander, ECF No. 102 (IP address listed: 96.3.75.15); Jeff Scherer, ECF No. 111 (IP address listed: 184.96.91.86); Erik E. Johnston, ECF No. 121 (No IP address listed); Leigh Norris, ECF No. 126 (No IP address listed); Michael Scott Davis, ECF No. 127 (No IP address listed); Neel N. Patel, ECF No. 130 (No IP address

affidavits or declarations attesting that they do not reside, transact or solicit business, or otherwise have sufficient contacts in the District of Columbia. These asserted facts would become relevant for the Court's consideration when and if these individuals are named as parties in this action. They cannot be dismissed, under Federal Rule of Civil Procedure 12(b)(2), from a lawsuit to which they are not parties.

Moreover, to establish personal jurisdiction, the Court must examine whether jurisdiction is applicable under the District of Columbia's long-arm statute, D.C. CODE § 13-423, and must also determine whether jurisdiction satisfies the requirements of due process. *See GTE New Media Servs. Inc. v. BellSouth Corp.*, 199 F.3d 1343, 1347 (D.C. Cir. 2000). Due Process requires the plaintiff to show that the defendant has "minimum contacts" with the forum, thereby ensuring that "the defendant's conduct and connection with the forum State are such that he should reasonably anticipate being haled into court there." *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286, 297 (1980); *see also GTE New Media Servs.*, 199 F.3d at 1347.

In cases where a party's contacts with the jurisdiction are unclear and the record before the court is "plainly inadequate," courts have allowed for a discovery period within which to gather evidence to support jurisdiction. *See GTE New Media Servs.*, 199 F.3d at 1351-52 (reversing lower court's finding of personal jurisdiction, but stating that "[t]his court has previously held that if a party demonstrates that it can supplement its jurisdictional allegations through discovery, then jurisdictional discovery is justified."). "This Circuit's standard for permitting jurisdictional discovery is quite liberal," *Diamond Chem. Co. v. Atofina Chems., Inc.*, 268 F. Supp. 2d 1, 15 (D.D.C. 2003), and jurisdictional discovery is available when a party has "at least a good faith belief" that it has personal jurisdiction. *Caribbean Broad. Sys., Ltd. v.*

listed); Matthew J. Selck, ECF No. 132 (No IP address listed); Aaron Tukey, ECF No. 136 (IP address listed: 68.116.170.119); J. McCarthy, ECF No. 148 (IP address listed: 72.73.239.68).

Cable & Wireless PLC, 148 F.3d 1080, 1090 (D.C. Cir. 1998). Courts have permitted discovery even when a party has failed to establish a *prima facie* case of personal jurisdiction. *See GTE New Media Servs.*, 199 F.3d at 1352 (“... as the record now stands, there is absolutely no merit to [plaintiff]’s bold claim that the parent companies and subsidiaries involved in this lawsuit should be treated identically. Jurisdictional discovery will help to sort out these matters.”); *see also In re Vitamins Antitrust Litigation*, 94 F. Supp. 2d 26, 35 (D.D.C. 2000) (discussing *GTE New Media Servs.* and stating that “the D.C. Circuit held that although plaintiffs had failed to establish a *prima facie* case of personal jurisdiction and the court was unable to tell whether jurisdictional discovery would assist GTE on this score, plaintiffs were entitled to pursue [discovery].”). In such cases, a party is entitled to pursue “precisely focused discovery aimed at addressing matters relating to personal jurisdiction.” *GTE New Media Servs.*, 199 F.3d at 1352.

Although the putative defendants assert that they do not have sufficient contacts with this jurisdiction to justify personal jurisdiction, the Court, as well as the plaintiff, has limited information to assess whether these jurisdictional defenses are valid¹⁸ and to evaluate possible alternate bases to establish jurisdiction. *See, e.g., London-Sire Records, Inc.*, 542 F. Supp. 2d at 181 (“Even taking all of the facts in [the putative defendant’s] affidavit as true, it is possible that the Court properly has personal jurisdiction.”); *Humane Soc’y of the United States v. Amazon.com, Inc.*, No. 07-623, 2007 U.S. Dist. LEXIS 31810, at *10 (D.D.C. May 1, 2007)

¹⁸ The putative defendants argue that the plaintiff should have used freely available tools that extract the geolocation information embedded in each IP address in order to verify the putative defendants’ location prior to filing claims in the District of Columbia. While it may behoove the plaintiff to utilize tools to ascertain the general location of the putative defendants prior to filing its case, these lookup tools are not completely accurate and it does not resolve for the Court the question of whether personal jurisdiction would be proper. Ultimately, the Court would still be unable to evaluate properly jurisdictional arguments until the putative defendants are identified and named. *See Sony*, 326 F. Supp. 2d at 567-68 (“Assuming personal jurisdiction were proper to consider at this juncture, the [publicly available IP lookup] techniques suggested by amici, at best, suggest the mere ‘likelihood’ that a number of defendants are located [outside this jurisdiction]. This, however, does not resolve whether personal jurisdiction would be proper.”).

(“[A] plaintiff faced with a motion to dismiss for lack of personal jurisdiction is entitled to reasonable discovery, lest the defendant defeat the jurisdiction of a federal court by withholding information on its contacts with the forum,” quoting *Virgin Records Am., Inc. v. Does 1-35*, No. 05-1918, 2006 WL 1028956, at *3 (D.D.C. Apr. 18, 2006)). To be clear, at this stage in the proceedings, the plaintiff is engaged in discovery to identify the proper defendants to be named in this lawsuit, including whether the exercise of jurisdiction over each potential defendant is proper. If and when the putative defendants are ultimately named in this lawsuit, the defendants will have the opportunity to file appropriate motions challenging the Court’s jurisdiction, and the Court will be able to evaluate personal jurisdiction defenses and consider dismissal. Until that time, however, dismissal under Rule 12(b)(2) is inappropriate.¹⁹ See *London-Sire Records*, 542 F. Supp. 2d at 180-181 (“premature to adjudicate personal jurisdiction” and permitting plaintiff to engage in jurisdictional discovery); *Sony*, 326 F. Supp. 2d. at 567-68 (same); *Virgin Records*, 2006 WL 1028956, at *3 (“Defendant’s Motion to Quash is without merit [] because it is premature to consider the question of personal jurisdiction in the context of a subpoena directed at determining the identity of the Defendant,” citing *Elektra Entm’t Grp., Inc. v. Does 1-9*, No. 04-2289, 2004 WL 2095581, at *5 (S.D.N.Y. Sept. 8, 2004); *UMG Recordings v. Does 1-199*, No. 04-0093, slip op. at 2 (D.D.C. Mar. 10, 2004)). Accordingly, the putative defendants’ motions to dismiss based on a purported lack of personal jurisdiction are denied at this time.

VI. CONCLUSION

For the reasons stated above, the putative defendants have failed to demonstrate that the plaintiff’s subpoenas issued to ISPs should be quashed, that protective orders are warranted, or

¹⁹ A more expansive discussion regarding the personal jurisdiction issues involved in this case is contained in the Court’s Memorandum Opinion filed March 22, 2011 in a similar case involving putative defendants accused of using the BitTorrent file-sharing technology to download and distribute illegally copyright works. See *Call of the Wild Movie, LLC v. Does 1-1,062*, No. 10-cv-455, 2011 WL 996786 at *7-10 (D.D.C. Mar. 22, 2011).

that the putative defendants should otherwise be dismissed from this case for improper joinder or a lack of personal jurisdiction. Accordingly, the following motions to quash the plaintiff's subpoenas, motions to be dismissed from the lawsuit, and motions for protective orders are denied: Jeff Kowalski, ECF No. 9 (No IP address listed); Janyth D. Girard, ECF No. 11 (IP address listed: 71.32.60146); Mark Richards, ECF No. 12 (IP address listed: 216.175.86.12); Matt Robinson, listed as John Doe, ECF No. 12 (IP address listed: 97.120.111.248); Blake Leverett, ECF No. 12 (IP address listed: 92.112.148.232); Salil Kadam, ECF No. 12 (IP address listed: 174.22.224.236); Margaret Wenzek, ECF No. 15 (No IP address listed); Audrey Kalblinger, ECF No. 16 (No IP address listed); Delmar R. Towler, ECF No. 18 (No IP address listed); JoNeane Key, ECF No. 18 (No IP address listed); Kenneth G. Kupke, ECF No. 18 (No IP address listed); John Doe, ECF No. 18 (IP address listed: 216.160.106.134); John Doe, ECF No. 18 (IP address listed: 67.40.214.85); John Doe, ECF No. 18 (No IP address listed); Richard L. Stelloh, ECF No. 18 (No IP address listed); Louis R. Carpenter, ECF No. 18 (IP address listed: 97.127.24.109); Nicole G. Lipson, ECF No. 18 (No IP address listed); Darcie Dikeman, ECF No. 21 (No IP address listed); John Doe, ECF No. 23 (IP address listed: 93.36.141.178); Jason Brittan, ECF No. 28 (No IP address listed); Sherry Porter, ECF No. 29 (No IP address listed); Mary Jo Elgie, ECF No. 30 (IP address listed: 98.118.130.44); James Kane, ECF No. 32 (No IP address listed); Jay R. Frydenlund, ECF No. 33 (IP address listed: 71.38.47.225); Debora L. Andrews, ECF No. 34 (IP address listed: 174.31.89.186); Jan H. Slater, ECF No. 35 (IP address listed: 71.21.25.157); Millwee Holler-Kanaga, ECF No. 36 (IP address listed: 75.165.182.92); Sara Sherwood, ECF No. 37 (IP address listed: 00:13:10:b9:71:a5); Ben Hatch, ECF No. 38 (No IP address listed); Sandra Dockery, ECF No. 39 (No IP address listed); Colin Quennell, ECF No. 40 (No IP address listed); William C. Cook, Sr., ECF No. 41 (IP address listed: 71.217.225.229);

Raghibir Singh, ECF No. 42 (IP address listed: 174.31.245.30); Corbin Swan, ECF No. 43 (No IP address listed); Arthur B. Cutting, ECF No. 44 (IP address listed: 174.26.9.140); A. Turner, ECF No. 45 (IP address listed: 216.161.89.109); LaMarr M. Jones, ECF No. 46 (No IP address listed); Richard DeHart, ECF No. 47 (IP address listed: 70.59.194.89); Byron Lee, ECF No. 48 (IP address listed: 96.40.190.149.00); Adam Delgado, ECF No. 49 (IP address listed: 24.177.13.76); Karen Eiriz, ECF No. 50 (No IP address listed); Lucy A. Marsh, ECF No. 53 (No IP address listed); Michael Koenig, ECF No. 54 (IP address listed: 173.71.1.125); Cheryl A. Lobo, ECF No. 56 (No IP address listed); Randall J. Azbill, Sr., ECF No. 57 (No IP address listed); John T. Krayner, ECF No. 58 (No IP address listed); Joseph M. Luria, ECF No. 59 (No IP address listed); Cameron J. Kennedy, ECF No. 60 (No IP address listed); Shey Davis, ECF No. 61 (No IP address listed); David Allan Doll, ECF No. 62 (No IP address listed); Jonathan D. Coleman, ECF No. 63 (No IP address listed); Matthew Cohen, ECF No. 64 (IP address listed: 98.117.43.70); Joseph M. Orovic, ECF No. 65 (No IP address listed); Rowena K. Cruz, ECF No. 66 (No IP address listed); Miriam Adelson, ECF No. 67 (No IP address listed); Antonio R. Hinton, ECF No. 68 (No IP address listed); Judy Collins, ECF No. 69 (No IP address listed); Kenneth Kantorowicz, ECF No. 70 (IP address listed: 98.127.67.128); Aran Bedarian, ECF No. 71 (IP address listed: 71.84.245.56); James Verdin, ECF No. 72 (IP address listed: 97.127.116.204); Nick Hartmann, ECF No. 73 (No IP address listed); Jomy Joseph, ECF No. 74 (No IP address listed); Jonathan T. Payne, ECF No. 75 (No IP address listed); Carman I. Goodrich, ECF No. 76 (No IP address listed); John C. Jacobson, ECF No. 77 (No IP address listed); Ruth Shih, ECF No. 78 (No IP address listed); Sean E. Ringle, ECF No. 79 (No IP address listed); Simone J. Johnson, ECF No. 80 (No IP address listed); Jordan C. Neptune, ECF No. 81 (No IP address listed); Warren M. Gehl, ECF No. 82 (No IP address listed); Eric M. Miller, ECF No. 83 (No IP

address listed); Richard T. Holbrook, II, ECF No. 84 (No IP address listed); Darren Choong Sik Hng, ECF No. 85 (No IP address listed); Todd D. Merrifield, ECF No. 86 (No IP address listed); Michael Carter, ECF No. 88-1 (IP address listed: 72.174.15.52); Chang Myers, listed as Jane Doe, ECF No. 88-2 (IP address listed: 173.71.142.170); Leanne Ferguson fka Leanne Brogdon, ECF No. 94 (No IP address listed); Amelia Cardenas, ECF No. 95 (No IP address listed); Amanda J. Quast, ECF No. 96 (No IP address listed); Randy L. Morton, ECF No. 97 (No IP address listed); David Raines, listed as John Doe, ECF No. 98 (IP address listed: 68.118.179.157); Morris Carrejo, ECF No. 99 (No IP address listed); Charles Ellsworth, ECF No. 100 (No IP address listed); Nanci Lam, represented by Michael S. Lee, Esq, ECF No. 101 (No IP address listed); Samuel Neuenschwander, ECF No. 102 (IP address listed: 96.3.75.15); Khaled Hamed, ECF No. 103 (IP address listed: 68.184.152.100); Anita M. Dorrance, ECF No. 104 (No IP address listed); Syed Mobeen, ECF No. 105 (No IP address listed); Chelsea Reitzner, ECF No. 106 (IP address listed: 24.183.109.103); Alan Stowers, ECF No. 107 (No IP address listed); Shani Myers, ECF No. 108 (No IP address listed); Darryl Godfrey, ECF No. 109 (IP address listed: 75.132.186.254); Michael B. Parker, ECF No. 110 (No IP address listed); Jeff Scherer, ECF No. 111 (IP address listed: 184.96.91.86); Justin Solem, ECF No. 112 (IP address listed: 66.188.193.94); Aleksandr Baga, ECF No. 113 (IP address listed: 24.17.133.177); Donna Lynk, ECF No. 115 (IP address listed: 68.10.91.194); Adam Ceschin, ECF No. 117 (IP address listed: 97.120.111.248); Adam Owensby, ECF No. 118 (No IP address listed); Kathryn Lanier, ECF No. 119 (No IP address listed); Erik E. Johnston, ECF No. 121 (No IP address listed); Leigh Norris, ECF No. 126 (No IP address listed); Michael Scott Davis, ECF No. 127 (No IP address listed); Matthew Alan O'Connell, ECF No. 128 (No IP address listed); Kathleen Gonzales, ECF No. 129 (No IP address listed); Neel N. Patel, ECF No. 130 (No IP address

listed); Nancy Schwarz, ECF No. 131 (No IP address listed); Matthew J. Selck, ECF No. 132 (No IP address listed); Von R. Arnst, ECF No. 133 (No IP address listed); Adrian Taylor Tuia, ECF No. 134 (No IP address listed); Mary Woods, ECF No. 135 (IP address listed: 75.137.118.90); Aaron Tukey, ECF No. 136 (IP address listed: 68.116.170.119); Guntars Rizis, ECF No. 137 (No IP address listed); Chris Queen, ECF No. 138 (No IP address listed); Kaylin Werth, ECF No. 139 (IP address listed: 71.89.27.95); Freightmen International, ECF No. 140 (No IP address listed); William White, ECF No. 141 (IP address listed: 66.190.77.95); J. McCarthy, ECF No. 148 (IP address listed: 72.73.239.68); Rita Shostak, ECF No. 149 (No IP address listed). An Order consistent with this Memorandum Opinion will be entered.

DATE: MAY 12, 2011

/s/ Beryl A. Howell
BERYL A. HOWELL
United States District Judge

Exhibit 14

to

Plaintiff's Response to Order to Show Cause - CV 10-04472 BZ

On The Cheap, LLC DBA Tru Filth, LLC v. Does 1-5011, Case No. CV 10-04472 BZ

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

MAVERICK ENTERTAINMENT GROUP,
INC.,

Plaintiff,

v.

DOES 1-2,115,

Defendants.

Civil Action No. 10-0569 (BAH)
Judge Beryl A. Howell

MEMORANDUM OPINION

Pending before the Court are motions to dismiss, quash, and for protective orders filed by sixty-six putative defendants.¹ These individuals have yet to be named as defendants in this case, but claim to have received notices from their Internet Service Providers (hereinafter “ISPs”) that plaintiff Maverick Entertainment Group, Inc. seeks their identifying information in connection with allegations in the Complaint that certain IP addresses used a file-sharing program called BitTorrent to download and distribute illegally the plaintiff’s copyrighted movies. These sixty-six

¹ Thirty-six individuals have filed motions representing that they are putative defendants in the instant lawsuit, but have not provided the IP addresses listed in the plaintiff’s Complaint that are allegedly associated with their computer use. *See* Robert A. Foster, ECF No. 12; Gundie Logan, ECF No. 20; Juanita Burger, ECF No. 37; Silvia R. Morgan, ECF No. 38; Theresa M. McNiff, ECF No. 39; Tyler Edwin Thomas, ECF No. 50; Granville Oral Barrett, ECF No. 51; Shedrika Power, ECF No. 52; Lian Oltean, ECF No. 53; Armando Liban, ECF No. 54; Nicholas Caruso, ECF No. 55; Brian Bunn, ECF No. 67; Robert Slade, ECF No. 68; Christian Murphy, ECF No. 69; Lucyna Kwasniak, ECF No. 76; John Feher, ECF No. 77; Janice A. Harmis, ECF No. 79; Keith E. Nickoles, ECF No. 80; Raymond M. Duran, ECF No. 81; Marc Mordechai Mandel, ECF No. 82; Shelia A. Torrance, ECF No. 83; Daniel & Richard Probinsky, ECF No. 84; Antonio Forte, ECF No. 85; Phillip Bourmes, ECF No. 89; Belton B. Raines, Jr., ECF No. 91; Felix Martinez, ECF No. 93; Linda White, ECF No. 94; Douglass Edward Oster, ECF No. 95; Jose Otero, ECF No. 105; Tonya R. Moody, ECF No. 107; Darrin Ross, ECF No. 108; Eric Peterkin, ECF No. 119; Felicia Martin, ECF No. 125; Christopher C. Murdock, ECF No. 127; Cathy Patterson, ECF No. 128. The Court therefore has no way of verifying that these individuals are indeed potential parties in this lawsuit. Regardless, however, the defenses and arguments they assert are identical to those proffered by other putative defendants.

putative defendants have filed motions and letters seeking to prevent disclosure of their identifying information and otherwise to secure dismissal from the lawsuit.² For the reasons set forth below, the putative defendants' motions to quash, dismiss, and for protective orders are denied.

I. BACKGROUND

On April 8, 2010, plaintiff Maverick Entertainment Group, Inc. filed a Complaint against unnamed individuals who allegedly used a file-sharing protocol called BitTorrent to illegally infringe plaintiff's copyrights in thirteen motion pictures: *Army of the Dead*, *Border Town 2009*, *Buds for Life*, *Demons at the Door*, *Holy Hustler*, *Jack Squad*, *Smile Pretty* (aka *Nasty*), *Stripper Academy*, *The Casino Job*, *The Clique* (aka *Death Clique*), *Too Saved*, *Treasure Raiders*, and *Trunk*. Compl. ¶¶ 3, 9, ECF No. 1. The plaintiff subsequently filed an Amended Complaint listing 4,350 putative defendants, who are identified only by their IP addresses. Am. Compl., Aug. 10, 2010, ECF No. 9. Given that the defendants in this case were unidentified at the time the plaintiff filed its Complaint, on April 19, 2010, the Court granted the plaintiff leave to subpoena ISPs to obtain identifying information for the putative defendants. Minute Order dated April 19, 2010 (Leon, J.); Order Granting Pl.'s Mot. for Leave to Take Disc. Prior to Rule 26(f) Conference, May 24, 2010, ECF No. 7 (Leon, J.). Specifically, the Court authorized the plaintiff to obtain "information sufficient to identify each Defendant, including name, current (and permanent) addresses, telephone numbers, e-mail addresses, and Media Access Control addresses." Order Granting the Pl.'s Mot. for Leave to Take Disc. Prior to Rule 26(f) Conference, May 24, 2010, ECF No. 7 (Leon, J.), at 1. This information was to be "used by the plaintiff solely for the

² The Court recognizes that "at least two" putative defendants (Jasmin Silva, ECF Nos. 56; Mark Benavides, ECF No. 92) have "substantially copied" and filed briefs prepared and submitted by attorney Eric J. Menhart on behalf of his five clients: Xiangping Xu (ECF No. 56), Lori Pearlman (ECF No. 58), Cedric Johnson (ECF Nos. 14, 60), Antonio Forte (ECF No. 85), and Darrin Ross (ECF No. 108). *See* Eric J. Menhart's Notice re: Unauthorized Copying of Brief, ECF No. 124. Like Mr. Menhart, the Court notes the "irony" of such actions in a lawsuit involving copyright infringement. *Id.*

purpose of protecting the plaintiff's rights as set forth in the complaint." *Id.* at 2.³

Since the Court approved expedited discovery, ISPs have provided identifying information for the putative defendants in response to the plaintiff's subpoenas on a rolling basis.⁴ Prior to providing the plaintiff with a putative defendant's identifying information, however, the ISPs sent notices to the putative defendants informing them of their right to challenge release of their information in this Court.⁵ On April 4, 2011, the Court directed the plaintiff, *inter alia*, to dismiss the putative defendants that it did not intend to sue.⁶ Order Denying Pl.'s Mot. for Approval of Disc., Apr. 4, 2011, ECF No. 74. On April 15, 2011, the plaintiff voluntarily dismissed 2,579 putative defendants for whom it had received identifying information but did not intend to sue in this Court. Pl.'s Notice of Voluntary Dismissal, Apr. 15, 2011, ECF No. 97. On April 20, 2011, the plaintiff filed its Second Amended Complaint, which lists 2,115 putative

³ On October 25, 2010, the Court issued an Order approving discovery for the putative defendants specifically listed on Exhibit A to the plaintiff's First Amended Complaint. Order, Oct. 25, 2010, ECF No. 11 (Leon, J.).

⁴ Pursuant to Federal Rule of Civil Procedure 4(m), the plaintiff was required to name and serve defendants by August 6, 2010, which is the date within 120 days of filing its original Complaint. On that day, plaintiff requested an additional 120 days to name and serve the defendants because the plaintiff had yet to receive identifying information for all defendants listed in the plaintiff's Amended Complaint. ECF No. 9. On September 30, 2010, the Court granted this motion *nunc pro tunc* by Minute Order, extending the plaintiff's time to name and serve to January 28, 2011. Minute Order dated Sept. 30, 2011 (Leon, J.). On February 23, 2011, the Court extended the plaintiff's time to name and serve *nunc pro tunc* from January 28, 2011 to April 29, 2011 because ISPs had yet to fully respond to the plaintiff's subpoenas. Minute Order dated Feb. 23, 2011. At a motions hearing held on March 1, 2011 regarding Time Warner Cable's Motion to Quash, ECF No. 18, the Court extended the plaintiff's time to name and serve to June 13, 2011. Transcript of Mot. Hearing, at 68, *Maverick Entm't Grp., Inc. v. Does 1-2,115*, No. 10-cv-569 (Mar. 1, 2011)

⁵ The Court's Order approving expedited discovery did not expressly order the plaintiff or ISPs to send notices to putative defendants before their identifying information was released in response to the subpoenas. Plaintiff's counsel, however, represents that a notice was attached to all subpoenas issued to ISPs for identifying information. Transcript of Mot. Hearing, at 50-51, *Maverick Entm't Grp., Inc. v. Does 1-2,115*, No. 10-cv-569 (Mar. 1, 2011) ("Every single subpoena we sent to an ISP has the [notice approved by Judge Collyer in *Achte/Neunte Boll Kino Beteiligungs GMBH & Co, KG v. Does 1-4,577*, No. 10-cv-00453 (D.D.C. July 22, 2010) (Minute Order approving Court-Directed Notice, ECF No. 36)] attached to it. And [ISP] Time Warner, I believe, reached an agreement on the form of that notice in Judge Collyer's court, and every single subpoena we sent since that date in every new case has that notice.").

⁶ The Court also granted the plaintiff leave to replace 783 putative defendants in this lawsuit with 783 new putative defendants through a Second Amended Complaint after ISP Time Warner Cable failed to preserve identifying information relating to those original putative defendants. Order Denying Pl.'s Mot. for Approval of Disc., Apr. 4, 2011, ECF No. 74.

defendants. Second Am. Compl., ECF No. 111. None of the putative defendants with pending motions were dismissed. Pl.'s Notice of Voluntary Dismissal, Apr. 15, 2011, ECF No. 97, at 2.

The Court is now presented with motions or letters from sixty-six putative defendants who seek to prevent disclosure of their identifying information or otherwise obtain dismissal from the lawsuit: fourteen putative defendants have filed motions in which they generally deny using BitTorrent to download and distribute the plaintiff's movies,⁷ fifty-four putative defendants have filed motions to quash under on FED. R. CIV. P. 45(c)(3),⁸ thirteen have filed motions to dismiss

⁷ See Jose M. Barroso, ECF No. 20 (No IP address listed); Cindy Tate, ECF No. 20 (IP address listed: 68.187.201.11); Marty Ingebretsen, ECF No. 20 (IP address listed: 75.135.157.00); Jane Doe, ECF No. 20 (IP address listed: 75.129.147.167); John Doe, ECF No. 20 (IP address listed: 68.191.210.134); Juanita Burger, ECF No. 37 (No IP address listed); Connie Atkinson, ECF No. 62 (No IP address listed); Rohan Green, ECF No. 64 (No IP address listed); Robert McGrath, ECF No. 65 (No IP address listed); Sanjay Patel, ECF No. 66 (IP address listed: 69.254.240.39); Tonya R. Moody, ECF No. 107 (No IP address listed); Elizabeth Herrmann, ECF No. 90 (IP address listed: 71.226.65.201); Belton B. Raines, Jr., ECF No. 91 (No IP address listed); Dianne J. Ashley, ECF No. 120 (IP address listed: 76.22.80.133).

⁸ See Cedric Johnson, ECF Nos. 14, 60 (IP address listed: 97.91.179.237); Jose M. Barroso, ECF No. 20 (No IP address listed); Lori Pearlman, ECF No. 58 (IP address listed: 68.62.35.244); Xiangping Xu a.k.a. Kevin Xu, ECF No. 56 (IP address listed: 67.170.234.17); Silvia R. Morgan, ECF No. 38 (No IP address listed); Theresa M. McNiff, ECF No. 39 (No IP address listed); Tyler Edwin Thomas, ECF No. 50 (No IP address listed); Granville Oral Barrett, ECF No. 51 (No IP address listed); Shedrika Power, ECF No. 52 (No IP address listed); Lian Oltean, ECF No. 53 (No IP address listed); Armando Liban, ECF No. 54 (No IP address listed); Nicholas Caruso, ECF No. 55 (No IP address listed); Connie Atkinson, ECF No. 62 (No IP address listed); Jimmy Santana, ECF No. 63 (No IP address listed); Rohan Green, ECF No. 64 (No IP address listed); Robert McGrath, ECF No. 65 (No IP address listed); Sanjay Patel, ECF No. 66 (IP address listed: 69.254.240.39); Brian Bunn, ECF No. 67 (No IP address listed); Robert Slade, ECF No. 68 (No IP address listed); Christian Murphy, ECF No. 69 (No IP address listed); Lucyna Kwasniak, ECF No. 76 (No IP address listed); Richard G. Scoza, ECF No. 78 (IP address listed: 69.249.32.138); Janice A. Harmis, ECF No. 79 (No IP address listed); Keith E. Nickoles, ECF No. 80 (No IP address listed); Raymond M. Duran, ECF No. 81 (No IP address listed); Marc Mordechai Mandel, ECF No. 82 (No IP address listed); Shelia A. Torrance, ECF No. 83 (No IP address listed); Daniel & Richard Probinsky, ECF No. 84 (No IP address listed); Antonio Forte, ECF No. 85 (No IP address listed); Elizabeth Herrmann, ECF No. 90 (IP address listed: 71.226.65.201); Belton B. Raines, Jr., ECF No. 91 (No IP address listed); Mark Benavides, ECF No. 92 (IP address listed: 98.197.169.162); Felix Martinez, ECF No. 93 (No IP address listed); Linda White, ECF No. 94 (No IP address listed); Douglass Edward Oster, ECF No. 95 (No IP address listed); Victoria Kristian, ECF No. 102 (IP address listed: 76.111.164.34); John Doe (IP address listed: 65.96.173.62) and John Doe (IP address listed: 24.128.252.215) represented by Tuna Mecit, Esq., ECF No. 103; Marie Sanchez, ECF No. 104 (IP address listed: 174.51.121.33); Jose Otero, ECF No. 105 (No IP address listed); Dana Wilkerson, ECF No. 106 (IP address listed: 69.136.194); Darrin Ross, ECF No. 108 (No IP address listed); Eric Peterkin, ECF No. 119 (No IP address listed); Dianne J. Ashley, ECF No. 120 (IP address listed: 76.22.80.133); Jane Doe represented by Emanuel J. Oakes, Jr., Esq., ECF No. 121, (IP address listed: 98.239.170.63); Jasmin Silva, ECF No. 123 (IP address listed: 24.6.177.153); Felicia Martin, ECF No. 125 (No IP address listed); Scott Cassel, ECF No. 126 (IP address listed: 67.161.196.74); Christopher C. Murdock, ECF No. 127 (No IP address listed); Cathy Patterson, ECF No. 128 (No IP address listed); Inna Shkrabak, ECF No. 129 (IP address listed: 24.18.48.58); Kamil Kierski, ECF Nos. 130, 132 (IP address listed: 98.217.10.245); Tom Ni, ECF No. 131 (IP address listed: 71.233.3.232).

asserting that the plaintiff has improperly joined the putative defendants,⁹ and forty-three putative defendants have filed motions to dismiss based on lack of personal jurisdiction.¹⁰ Additionally, thirty-three putative defendants have filed motions for protective orders.¹¹ For the reasons stated

⁹ See Cedric Johnson, ECF Nos. 14, 60 (IP address listed: 97.91.179.237); Lori Pearlman, ECF Nos. 34, 58 (IP address listed: 68.62.35.244); Xiangping Xu a.k.a. Kevin Xu, ECF Nos. 35, 56 (IP address listed: 67.170.234.17); Daniel & Richard Probinsky, ECF No. 84 (No IP address listed); Antonio Forte, ECF No. 85 (No IP address listed); Mark Benavides, ECF No. 92 (IP address listed: 98.197.169.162); Darrin Ross, ECF No. 108 (No IP address listed); Jane Doe represented by Emanuel J. Oakes, Jr., Esq., ECF No. 121, (IP address listed: 98.239.170.63); Jasmin Silva, ECF No. 123 (IP address listed: 24.6.177.153); Inna Shkrabak, ECF No. 129 (IP address listed: 24.18.48.58); Kamil Kierski, ECF Nos. 130, 132 (IP address listed: 98.217.10.245); Tom Ni, ECF No. 131 (IP address listed: 71.233.3.232).

¹⁰ See Cedric Johnson, ECF Nos. 14, 60 (IP address listed: 97.91.179.237); Lori Pearlman, ECF No. 58 (IP address listed: 68.62.35.244); Xiangping Xu a.k.a. Kevin Xu, ECF No. 56 (IP address listed: 67.170.234.17); Silvia R. Morgan, ECF No. 38 (No IP address listed); Theresa M. McNiff, ECF No. 39 (No IP address listed); Tyler Edwin Thomas, ECF No. 50 (No IP address listed); Granville Oral Barrett, ECF No. 51 (No IP address listed); Shedrika Power, ECF No. 52 (No IP address listed); Lian Oltean, ECF No. 53 (No IP address listed); Armando Liban, ECF No. 54 (No IP address listed); Nicholas Caruso, ECF No. 55 (No IP address listed); Brian Bunn, ECF No. 67 (No IP address listed); Robert Slade, ECF No. 68 (No IP address listed); Christian Murphy, ECF No. 69 (No IP address listed); Lucyna Kwasniak, ECF No. 76 (No IP address listed); Richard G. Scoza, ECF No. 78 (IP address listed: 69.249.32.138); Janice A. Harmis, ECF No. 79 (No IP address listed); Keith E. Nickoles, ECF No. 80 (No IP address listed); Raymond M. Duran, ECF No. 81 (No IP address listed); Marc Mordechai Mandel, ECF No. 82 (No IP address listed); Shelia A. Torrance, ECF No. 83 (No IP address listed); Daniel & Richard Probinsky, ECF No. 84 (No IP address listed); Antonio Forte, ECF No. 85 (No IP address listed); Mark Benavides, ECF No. 92 (IP address listed: 98.197.169.162); Felix Martinez, ECF No. 93 (No IP address listed); Linda White, ECF No. 94 (No IP address listed); Douglass Edward Oster, ECF No. 95 (No IP address listed); Victoria Kristian, ECF No. 102 (IP address listed: 76.111.164.34); John Doe (IP address listed: 65.96.173.62) and John Doe (IP address listed: 24.128.252.215) represented by Tuna Mecit, Esq., ECF No. 103; Marie Sanchez, ECF No. 104 (IP address listed: 174.51.121.33); Jose Otero, ECF No. 105 (No IP address listed); Darrin Ross, ECF No. 108 (No IP address listed); Jane Doe represented by Emanuel J. Oakes, Jr., Esq., ECF No. 121, (IP address listed: 98.239.170.63); Jasmin Silva, ECF No. 123 (IP address listed: 24.6.177.153); Felicia Martin, ECF No. 125 (No IP address listed); Scott Cassel, ECF No. 126 (IP address listed: 67.161.196.74); Christopher C. Murdock, ECF No. 127 (No IP address listed); Cathy Patterson, ECF No. 128 (No IP address listed); Inna Shkrabak, ECF No. 129 (IP address listed: 24.18.48.58); Kamil Kierski, ECF Nos. 130, 132 (IP address listed: 98.217.10.245); Tom Ni, ECF No. 131 (IP address listed: 71.233.3.232).

¹¹ See Silvia R. Morgan, ECF No. 38 (No IP address listed); Theresa M. McNiff, ECF No. 39 (No IP address listed); Tyler Edwin Thomas, ECF No. 50 (No IP address listed); Granville Oral Barrett, ECF No. 51 (No IP address listed); Shedrika Power, ECF No. 52 (No IP address listed); Lian Oltean, ECF No. 53 (No IP address listed); Armando Liban, ECF No. 54 (No IP address listed); Nicholas Caruso, ECF No. 55 (No IP address listed); Brian Bunn, ECF No. 67 (No IP address listed); Robert Slade, ECF No. 68 (No IP address listed); Christian Murphy, ECF No. 69 (No IP address listed); Lucyna Kwasniak, ECF No. 76 (No IP address listed); John Feher, ECF No. 77 (No IP address listed); Richard G. Scoza, ECF No. 78 (IP address listed: 69.249.32.138); Janice A. Harmis, ECF No. 79 (No IP address listed); Keith E. Nickoles, ECF No. 80 (No IP address listed); Raymond M. Duran, ECF No. 81 (No IP address listed); Marc Mordechai Mandel, ECF No. 82 (No IP address listed); Shelia A. Torrance, ECF No. 83 (No IP address listed); Felix Martinez, ECF No. 93 (No IP address listed); Linda White, ECF No. 94 (No IP address listed); Douglass Edward Oster, ECF No. 95 (No IP address listed); Victoria Kristian, ECF No. 102 (IP address listed: 76.111.164.34); John Doe (IP address listed: 65.96.173.62) and John Doe (IP address listed: 24.128.252.215) represented by Tuna Mecit, Esq., ECF No. 103; Marie Sanchez, ECF No. 104 (IP address listed: 174.51.121.33); Jose Otero, ECF No. 105 (No IP address listed); Felicia Martin, ECF No. 125 (No IP address listed); Scott Cassel,

below, the Court denies all of these motions.

II. MOTIONS TO QUASH UNDER FEDERAL RULE OF CIVIL PROCEDURE 45

Fifty-two putative defendants have filed motions to quash the plaintiff's subpoenas issued to ISPs for the putative defendants' identifying information. These motions assert three arguments: First, the putative defendant filing the motion did not engage in the alleged illegal conduct and the plaintiff should therefore be prevented from obtaining the putative defendant's identifying information. Second, the subpoena should be quashed because it "requires disclosure of privileged or other protected matter" under FED. R. CIV. P. 45(c)(3)(A)(iii). Third, the plaintiff's subpoenas subject the putative defendant filing the motion to an undue burden under FED. R. CIV. P. 45(c)(3)(A)(iv). All of these arguments are unavailing.

Under Federal Rule of Civil Procedure 45(c), the Court must quash a subpoena when, *inter alia*, it "requires disclosure of privileged or other protected matter, if no exception or waiver applies" or "subjects a person to undue burden." FED. R. CIV. P. 45(c)(3)(A)(iii)-(iv). A general denial of engaging in copyright infringement is not a basis for quashing the plaintiff's subpoena. It may be true that the putative defendants who filed motions and letters denying that they engaged in the alleged conduct did not illegally infringe the plaintiff's copyrighted movies, and the plaintiff may, based on its evaluation of their assertions, decide not to name these individuals as parties in this lawsuit. On the other hand, the plaintiff may decide to name them as defendants in order to have an opportunity to contest the merits and veracity of their defenses in this case. In other words, if these putative defendants are named as defendants in this case, they

ECF No. 126 (IP address listed: 67.161.196.74); Christopher C. Murdock, ECF No. 127 (No IP address listed); Cathy Patterson, ECF No. 128 (No IP address listed); Kamil Kierski, ECF Nos. 130, 132 (IP address listed: 98.217.10.245); Tom Ni, ECF No. 131 (IP address listed: 71.233.3.232).

may deny allegations that they used BitTorrent to download and distribute illegally the plaintiff's movies, present evidence to corroborate that defense, and move to dismiss the claims against them. A general denial of liability, however, is not a basis for quashing the plaintiff's subpoenas and preventing the plaintiff from obtaining the putative defendants' identifying information. That would deny the plaintiff access to the information critical to bringing these individuals properly into the lawsuit to address the merits of both the plaintiff's claim and their defenses. *See Achte/Neunte Boll Kino Beteiligungs GMBH & Co, KG v. Does 1-4*, 577, 736 F. Supp. 2d 212, 215 (D.D.C. 2010) (denying motions to quash filed by putative defendants in BitTorrent file-sharing case and stating that putative defendants' "denial of liability may have merit, [but] the merits of this case are not relevant to the issue of whether the subpoena is valid and enforceable. In other words, they may have valid defenses to this suit, but such defenses are not at issue [before the putative defendants are named parties]."); *see also Fonovisa, Inc. v. Does 1-9*, No. 07-1515, 2008 WL 919701, at *8 (W.D. Pa. Apr. 3, 2008) (if a putative defendant "believes that it has been improperly identified by the ISP, [the putative defendant] may raise, at the appropriate time, any and all defenses, and may seek discovery in support of its defenses.").

Nine putative defendants urge the Court to quash the plaintiff's subpoenas based upon their privacy interests.¹² Rule 45(c)(3)(A)(iii) instructs a Court to quash a subpoena if it "requires disclosure of privileged or other protected matter." FED. R. CIV. P. 45(c)(3)(A)(iii). This rule, however, does not apply here. The Court recognizes that the putative defendants' First Amendment right to anonymous speech is implicated by disclosure of their identifying

¹² *See* Robert A. Foster, ECF No. 12 (No IP address listed); Gundie Logan, ECF No. 20 (No IP address listed); Cindy Tate, ECF No. 20 (IP address listed: 68.187.201.11); Marty Ingebretsen, ECF No. 20 (IP address listed: 75.135.157.00); Jane Doe, ECF No. 20 (IP address listed: 75.129.147.167); John Doe, ECF No. 20 (IP address listed: 68.191.210.134); Juanita Burger, ECF No. 37 (No IP address listed); Phillip Bournes, ECF No. 89 (No IP address listed); Mary Woods, ECF No. 109 (IP address listed: 75.137.118.90).

information. *See Sony Music Entm't, Inc. v. Does 1-40*, 326 F. Supp. 2d 556, 564 (S.D.N.Y. 2004) (“the file sharer may be expressing himself or herself through the music selected and made available to others.”); *see also London-Sire Records, Inc. v. Doe 1*, 542 F. Supp. 2d 153, 163 (D. Mass. 2008). Nevertheless, whatever asserted First Amendment right to anonymity the putative defendants may have in this context does not shield them from allegations of copyright infringement.¹³ *See Arista Records LLC v. Does 1-19*, 551 F. Supp. 2d 1, 8 (D.D.C. 2008) (“First Amendment privacy interests are exceedingly small where the ‘speech’ is the alleged infringement of copyrights.”); *Achte/Neunte*, 736 F. Supp. 2d at 216 n.2 (“the protection afforded to such speech is limited and gives way in the face of a prima facie showing of copyright infringement”); *West Bay One, Inc. v. Does 1-1653*, 270 F.R.D. 13, 16 n.4 (D.D.C. 2010) (same); *Sony*, 326 F. Supp. 2d at 567 (First Amendment right of alleged file-sharers to remain anonymous “must give way to the plaintiffs’ right to use the judicial process to pursue what appear to be meritorious copyright infringement claims.”); *Elektra Entm’t Grp., Inc. v. Does 1-9*, No. 04-2289, 2004 WL 2095581, at *4-5 (S.D.N.Y. Sept. 8, 2004) (finding that First Amendment right to anonymity is overridden by plaintiff’s right to protect copyright).

Finally, the argument that the plaintiff’s subpoenas subject putative defendants to an undue burden is also unavailing. Putative defendants essentially argue that the plaintiff’s subpoenas require them to litigate in a forum in which they should not be subject to personal jurisdiction, which causes them hardship. As explained more fully *infra*, the putative defendants’ personal jurisdiction arguments are premature at this time because they have not

¹³ A more expansive discussion of the putative defendants’ First Amendment rights in this case is contained in the Court’s Memorandum Opinion filed March 22, 2011, which addresses amici Electronic Frontier Foundation, Public Citizen, American Civil Liberties Union Foundation, American Civil Liberties Union of the Nation’s Capital’s contention that the putative defendants’ First Amendment rights protect against disclosure of the putative defendants’ identifying information. *Call of the Wild Movie, LLC v. Does 1-1,062*, No. 10-cv-455, 2011 WL 996786 at *10-15 (D.D.C. Mar. 22, 2011) (consolidated opinion also addressing motions filed in *Maverick Entm’t Grp., Inc. v. Does 2,115*, No. 10-cv-569).

been named as parties to this lawsuit. Given that they are not named parties, the putative defendants are not required to respond to the allegations presented in the plaintiff's Second Amended Complaint or otherwise litigate in this district. The plaintiff has issued subpoenas to the putative defendants' ISPs, not to the putative defendants themselves. Consequently, the putative defendants face no obligation to produce any information under the subpoenas issued to their respective ISPs and cannot claim any hardship, let alone undue hardship.¹⁴

The plaintiff's subpoenas requesting the putative defendants' identifying information do not subject the putative defendants to an undue burden nor is the plaintiff's request for the information outweighed by any privacy interest or First Amendment right to anonymity. Moreover, a general denial of liability is not a proper basis to quash the plaintiff's subpoenas. Accordingly, the putative defendants' motions, under Federal Rule of Civil Procedure 45(c)(3), to quash the subpoenas are denied.

III. MOTIONS FOR PROTECTIVE ORDERS

Thirty-three putative defendants have filed motions for protective orders seeking to protect their identities from being disclosed to the plaintiff.¹⁵ Rule 26(c) provides that a court

¹⁴ Any reliance the putative defendants may have placed on Federal Rule of Civil Procedure 45(c)(3)(A)(ii) as an alternate basis for quashing the plaintiff's subpoenas is therefore also misplaced. Rule 45(c)(3)(A)(ii) requires the Court to quash a subpoena when the subpoena "requires a person who is neither a party nor a party's officer to travel more than 100 miles from where that person resides, is employed, or regularly transacts business in person" The putative defendants are not required to respond to the plaintiff's subpoenas or otherwise travel away from their homes or places of employment.

¹⁵ See Silvia R. Morgan, ECF No. 38 (No IP address listed); Theresa M. McNiff, ECF No. 39 (No IP address listed); Tyler Edwin Thomas, ECF No. 50 (No IP address listed); Granville Oral Barrett, ECF No. 51 (No IP address listed); Shedrika Power, ECF No. 52 (No IP address listed); Lian Oltean, ECF No. 53 (No IP address listed); Armando Liban, ECF No. 54 (No IP address listed); Nicholas Caruso, ECF No. 55 (No IP address listed); Brian Bunn, ECF No. 67 (No IP address listed); Robert Slade, ECF No. 68 (No IP address listed); Christian Murphy, ECF No. 69 (No IP address listed); Lucyna Kwasniak, ECF No. 76 (No IP address listed); John Feher, ECF No. 77 (No IP address listed); Richard G. Scoza, ECF No. 78 (IP address listed: 69.249.32.138); Janice A. Harmis, ECF No. 79 (No IP address listed); Keith E. Nickoles, ECF No. 80 (No IP address listed); Raymond M. Duran, ECF No. 81 (No IP address listed); Marc Mordechai Mandel, ECF No. 82 (No IP address listed); Shelia A. Torrance, ECF No. 83 (No IP address listed); Felix Martinez, ECF No. 93 (No IP address listed); Linda White, ECF No. 94 (No IP address listed); Douglass Edward Oster, ECF No. 95 (No IP address listed); Victoria Kristian, ECF No. 102 (IP address listed: 76.111.164.34); John Doe (IP address listed: 65.96.173.62) and John Doe (IP address listed: 24.128.252.215)

may “issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense.” FED. R. CIV. P. 26(c)(1).¹⁶ Such protective orders may forbid disclosure altogether, or, among other measures, “limit[] the scope of disclosure or discovery to certain matters.” FED. R. CIV. P. 26(c)(1)(A) and (D). “[A]lthough Rule 26(c) contains no specific reference to privacy or to other rights or interests that may be implicated, such matters are implicit in the broad purpose and language of the Rule.” *In re Sealed Case (Medical Records)*, 381 F.3d 1205, 1215 (D.C. Cir. 2004) (quoting *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 35 n.21 (1984)).

As elaborated above, the putative defendants are not subject to the plaintiff’s subpoenas, and therefore do not face any “annoyance, embarrassment, oppression, or undue burden or expense” from the plaintiff’s discovery request. *See* FED. R. CIV. P. 26(c)(1). To the extent that the putative defendants seek protective orders to prevent disclosure of private identifying information, the Court has held that the putative defendants’ First Amendment rights to anonymity in the context of their BitTorrent activity is minimal and outweighed by the plaintiff’s need for the putative defendants’ identifying information in order to protect its copyrights. *See Call of the Wild Movie, LLC v. Does 1-1,062*, No. 10-cv-455, 2011 WL 996786 at *10-15 (D.D.C. Mar. 22, 2011). The putative defendants’ requests for protective orders are therefore denied.

represented by Tuna Mecit, Esq., ECF No. 103; Marie Sanchez, ECF No. 104 (IP address listed: 174.51.121.33); Jose Otero, ECF No. 105 (No IP address listed); Felicia Martin, ECF No. 125 (No IP address listed); Scott Cassel, ECF No. 126 (IP address listed: 67.161.196.74); Christopher C. Murdock, ECF No. 127 (No IP address listed); Cathy Patterson, ECF No. 128 (No IP address listed); Kamil Kierski, ECF Nos. 130, 132 (IP address listed: 98.217.10.245); Tom Ni, ECF No. 131 (IP address listed: 71.233.3.232). The Court directed the Clerk to file these motions under seal pending resolution of their motions for protective orders. The Court denies these motions in the instant Memorandum Opinion, and, as reflected in the Order accompanying this Memorandum Opinion, the Clerk is directed to unseal the ECF docket entries 38-39, 50-55, 67-69, 76-83, 93-95, 102-05, 125-28, 130-132.

¹⁶ Many of the putative defendants state that they seek protective orders pursuant to Federal Rule of Civil Procedure 37. The Court assumes, however, that they seek protective orders under Federal Rule of Civil Procedure 26(c), and construes their motions accordingly.

IV. MOTIONS TO DISMISS BASED ON IMPROPER JOINDER

Thirteen putative defendants argue that they should be dismissed from the lawsuit because the plaintiff has improperly joined them with other putative defendants.¹⁷ The putative defendants' argument that they are improperly joined may be meritorious should they be named as defendants in this action. At this stage in the litigation, however, when discovery is underway to learn identifying facts necessary to permit service on Doe defendants, joinder, under Federal Rule of Civil Procedure 20(a)(2), of unknown parties identified only by IP addresses is proper. As discussed below, this conclusion is further supported by the allegations set forth in the Complaint, which sufficiently establishes a *prima facie* case of infringement of plaintiff's copyrights by users of the same file-sharing software program that operates through simultaneous and sequential computer connections and data transfers among the users.

At the outset, the Court notes that the remedy for improper joinder under Federal Rule of Civil Procedure 21 is not dismissal of the action.¹⁸ FED. R. CIV. P. 21 ("Misjoinder of parties is not a ground for dismissing an action."). Improper joinder may be remedied by "drop[ping]" a party and severing claims against that party. FED. R. CIV. P. 21 ("On motion or on its own, the

¹⁷ See Cedric Johnson, ECF Nos. 14, 60 (IP address listed: 97.91.179.237); Lori Pearlman, ECF Nos. 34, 58 (IP address listed: 68.62.35.244); Xiangping Xu a.k.a. Kevin Xu, ECF Nos. 35, 56 (IP address listed: 67.170.234.17); Daniel & Richard Probinsky, ECF No. 84 (No IP address listed); Antonio Forte, ECF No. 85 (No IP address listed); Mark Benavides, ECF No. 92 (IP address listed: 98.197.169.162); Darrin Ross, ECF No. 108 (No IP address listed); Jane Doe represented by Emanuel J. Oakes, Jr., Esq., ECF No. 121, (IP address listed: 98.239.170.63); Jasmin Silva, ECF No. 123 (IP address listed: 24.6.177.153); Inna Shkrabak, ECF No. 129 (IP address listed: 24.18.48.58); Kamil Kierski, ECF Nos. 130, 132 (IP address listed: 98.217.10.245); Tom Ni, ECF No. 131 (IP address listed: 71.233.3.232).

¹⁸ Rule 21 does not set forth what constitutes misjoinder, but "it is well-settled that parties are misjoined when the preconditions of permissive joinder set forth in Rule 20(a) have not been satisfied." *Disparte v. Corporate Exec. Bd.*, 223 F.R.D. 7, 12 (D.D.C. 2004) (citation omitted). Courts have also read Rule 21 in conjunction with Rule 42(b), which allows the court to sever claims in order to avoid prejudice to any party. *M.K. v. Tenet*, 216 F.R.D. 133, 138 (D.D.C. 2002); see also FED. R. CIV. P. 42(b) ("For convenience, to avoid prejudice, or to expedite and economize, the court may order a separate trial of one or more separate issues, claims, crossclaims, counterclaims, or third-party claims."). In addition to the two requirements of Rule 20(a)(2), courts therefore also consider whether joinder would prejudice any party or result in needless delay. See *Lane v. Tschetter*, No. 05-1414, 2007 WL 2007493, at *7 (D.D.C. July 10, 2007); *Tenet*, 216 F.R.D. at 138.

Court may at any time, on just terms, add or drop a party.”). This would simply create separate actions containing the same claims against the same putative defendants. *See Bailey v. Fulwood*, No. 10-463, 2010 U.S. Dist. LEXIS 141356, at *11 (D.D.C. Feb. 15, 2010); *In re Brand-Name Prescription Drugs Antitrust Litig.*, 264 F. Supp. 2d 1372, 1376 (J.P.M.L. 2003) (“[S]everance of claims under Rule 21 results in the creation of separate actions.”). The Court may exercise discretion regarding the proper time to sever parties, and this determination includes consideration of judicial economy and efficiency. *See Disparte v. Corporate Exec. Bd.*, 223 F.R.D. 7, 10 (D.D.C. 2004) (Permissive joinder under Federal Rule 20 is designed “to promote trial convenience and expedite the resolution of lawsuits,” quoting *Puricelli v. CNA Ins. Co.*, 185 F.R.D. 139, 142 (N.D.N.Y. 1999)). For example, in *London-Sire Records, Inc. v. Doe 1*, 542 F. Supp. 2d 153 (D. Mass. 2008), the court consolidated separate Doe lawsuits for copyright infringement since the “cases involve[d] similar, even virtually identical, issues of law and fact: the alleged use of peer-to-peer software to share copyrighted sound recordings and the discovery of defendants’ identities through the use of a Rule 45 subpoena to their internet service provider.” *Id.* at 161. In the court’s view, consolidation of the separate lawsuits for purposes of expedited discovery “ensures administrative efficiency for the Court, the plaintiffs, and the ISP, and allows the defendants to see the defenses, if any, that other John Does have raised.” *Id.* The court noted that, after discovery, “[t]he case against each Doe [would] be individually considered for purposes of any rulings on the merits,” and the putative defendants could “renew the severance request before trial if the case proceeds to that stage.” *Id.* at 161 n.7.

In addition to providing efficiencies for expedited discovery on jurisdictional issues, defendants may be properly joined in one action when claims arise from the same transaction or occurrence or series of transactions or occurrences; and any question of law or fact in the action

is common to all defendants. FED. R. CIV. P. 20(a)(2); *see also Montgomery v. STG Int'l, Inc.*, 532 F. Supp. 2d 29, 35 (D.D.C. 2008) (interpreting Rule 20(a)(1), which has the same requirements as Rule 20(a)(2)). The requirements for permissive joinder are “liberally construed in the interest of convenience and judicial economy in a manner that will secure the just, speedy, and inexpensive determination of the action.” *Lane v. Tschetter*, No. 05-1414, 2007 WL 2007493, at *7 (D.D.C. July 10, 2007) (internal quotation omitted); *see also Davidson v. District of Columbia*, 736 F. Supp. 2d 115, 119 (D.D.C. 2010). Thus, “the impulse is toward entertaining the broadest possible scope of action consistent with fairness to the parties; [and] joinder of claims, parties, and remedies is strongly encouraged.” *United Mine Workers of Am. v. Gibbs*, 383 U.S. 715, 724 (1966).

In the present case, the plaintiff has met all the requirements for permissive joinder under Federal Rule of Civil Procedure 20(a)(2). The first requirement is that claims must “aris[e] out of the same transaction, occurrence, or series of transactions or occurrences.” FED. R. CIV. P. 20(a)(2)(A). This essentially requires claims asserted against joined parties to be “logically related.” *Disparte*, 223 F.R.D. at 10. This is a flexible test and courts seek the “broadest possible scope of action.” *Lane*, 2007 WL 2007493, at *7 (quoting *Gibbs*, 383 U.S. at 724).

The plaintiff alleges that the putative defendants used the BitTorrent file-sharing protocol to distribute illegally the plaintiff’s motion pictures. Second Am. Compl., ¶¶ 3, 9-11. This file-sharing protocol “makes every downloader also an uploader of the illegally transferred file(s). This means that every . . . user who has a copy of the infringing copyrighted material on a torrent network must necessarily also be a source of download for that infringing file.” *Id.* at ¶ 3. The plaintiff further asserts that the “nature of a BitTorrent protocol [is that] any seed peer that has downloaded a file prior to the time a subsequent peer downloads the same file is automatically a

source for the subsequent peer so long as that first seed peer is online at the time the subsequent peer downloads a file.” *Id.* at ¶ 4.

Based on these allegations, the plaintiff’s claims against the putative defendants are logically related at this stage in the litigation. According to the plaintiff, each putative defendant is a possible source for the plaintiff’s motion pictures, and may be responsible for distributing the motion pictures to the other putative defendants, who are also using the same file-sharing protocol to copy the copyrighted material. *See Disparte*, 223 F.R.D. at 10 (to satisfy Rule 20(a)(2)(A) claims must be “logically related” and this test is “flexible.”). While the putative defendants may be able to rebut these allegations at a later date, at this procedural juncture the plaintiff has sufficiently alleged that its claims against the putative defendants potentially stem from the same transaction or occurrence, and are logically related. *See Arista Records LLC v. Does 1-19*, 551 F. Supp. 2d 1, 11 (D.D.C. 2008) (“While the Courts notes that the remedy for improper joinder is severance and not dismissal, the Court also finds that this inquiry is premature without first knowing Defendants’ identities and the actual facts and circumstances associated with Defendants’ conduct.” (internal citation omitted)).

Some courts in other jurisdictions have granted motions by putative defendants for severance in analogous copyright infringement cases against unknown users of peer-to-peer file-sharing programs for failure to meet the “same transaction or occurrence test” in Rule 20(a)(2). Those courts have been confronted with bare allegations that putative defendants used the same peer-to-peer network to infringe copyrighted works and found those allegations were insufficient for joinder. *See, e.g., IO Grp., Inc. v. Does 1-19*, No. 10-03851, 2010 WL 5071605, at *8-12 (N.D. Cal. Dec. 7, 2010); *Arista Records, LLC v. Does 1-11*, No. 07-cv-2828, 2008 WL 4823160, at *6 (N.D. Ohio Nov. 3, 2008) (“merely alleging that the Doe Defendants all used the

same ISP and file-sharing network to conduct copyright infringement without asserting that they acted in concert was not enough to satisfy the same series of transactions requirement under the Federal Rules.”); *LaFace Records, LLC v. Does 1-38*, No. 5:07-cv-298, 2008 WL 544992, at *3 (E.D. N.C. Feb. 27, 2008) (severing putative defendants in file-sharing case not involving BitTorrent technology, noting that “other courts have commonly held that where there is no assertion that multiple defendants have acted in concert, joinder is improper.”); *Interscope Records v. Does 1-25*, No. 6:04-cv-197, 2004 U.S. Dist. LEXIS 27782 (M.D. Fla. Apr. 1, 2004) (adopting Mag. J. Report and Recommendation at *Interscope Records v. Does 1-25*, No. 6:04-cv-197, 2004 U.S. Dist. LEXIS 27782 (M.D. Fla. Apr. 1, 2004)). That is not the case here.

The plaintiff has provided detailed allegations about how the BitTorrent technology differs from other peer-to-peer file-sharing protocols and necessarily engages many users simultaneously or sequentially to operate. *See Columbia Pictures Indus. v. Fung*, No. 06-5578, 2009 U.S. Dist. LEXIS 122661, at *7 (C.D. Cal. Dec. 21, 2009) (BitTorrent “is unique from that of previous [P2P] systems such as Napster and Grokster. Rather than downloading a file from an individual user, [BitTorrent users download] from a number of host computers that possess the file simultaneously. . . . The BitTorrent client application [] simultaneously downloads the pieces of the content file from as many users as are available at the time of the request, and then reassembles the content file on the requesting computer when the download is complete. Once a user downloads a given content file, he also becomes a source for future requests and downloads.”). Specifically, BitTorrent creates a “swarm” in which “each additional user becomes a part of the network from where the file can be downloaded . . . [U]nlike a traditional peer-to-peer network, each new file downloader is receiving a different piece of the data from each user who has already downloaded the file that together comprises the whole.” Second Am.

Compl., ¶ 3.

At least one court has not been persuaded that allegations of copyright infringement by users of BitTorrent satisfy the requirement of Rule 20. *See, e.g., Lightspeed v. Does 1-1000*, No. 10-cv-5604, 2011 U.S. Dist. LEXIS 35392, at *4-7 (N.D. Ill. Mar. 31, 2011) (finding that Doe defendants using BitTorrent technology were misjoined on the basis that the putative defendants were not involved in the “same transaction, occurrence, or series of transactions or occurrence” under FED. R. CIV. P. 20(a)(2)(A)); *Millennium TGA Inc. v. Does 1-800*, No. 10-cv-5603, 2011 U.S. Dist. LEXIS 35406, at *3-5 (N.D. Ill. Mar. 31, 2011) (same). In those cases, the court did not discuss the precise nature of the BitTorrent technology, which enables users to contribute to each other’s infringing activity of the same work as part of a “swarm.” Similarly to the instant claims of infringement of thirteen copyrighted works by the putative defendants, the plaintiffs in *Lightspeed* and *Millennium TGA Inc.* alleged infringement of multiple works. Indeed, concluding that the allegations against the putative defendants in this case stem from the same transaction, or series of transactions is made more complicated by the fact that the plaintiff claims infringement of thirteen separate movies. This is a factor that may undermine the requisite showing of concerted activity to support joinder when the plaintiff identifies and names defendants to this action. *See Fonovisa, Inc. v. Does 1-9*, 2008 WL 919701, at *6 (W. D. Pa. April 3, 2008)(Misjoinder found in copyright infringement case where “[n]one of the Defendants downloaded and/or distributed the same copyrighted recordings belonging to the same set of Plaintiffs, and each of the Defendants accessed a different number of audio files on different dates); *See Bridgeport Music, Inc. v. IIC Music*, 202 F.R.D. 229, 232 (M.D. Tenn. 2001) (severing defendants accused of sampling different songs and stating that sampling of each song represented a “discrete occurrence” and that “the Court is not persuaded by Plaintiffs’ argument

that its infringement counts are properly joined because Plaintiffs suffered the same harm in each instance. According to this logic, a copyright plaintiff could join as defendants any otherwise unrelated parties who independently copy material owned by the plaintiff.”). The Court is guided, however, by the principle that permissive joinder seeks the “broadest possible scope of action,” *Gibbs*, 383 U.S. at 724, particularly when there are no named defendants and the putative defendants are not harmed by joinder at this stage. Should the defendants be named and make motions for severance, the plaintiff will be required to demonstrate with greater specificity the relatedness of the named defendants’ alleged conduct and the factual basis for joinder under Rule 20(a)(2)(A).

The second requirement for proper joinder under Rule 20(a)(2) is that the plaintiff’s claims against the putative defendants must contain a common question of law or fact. FED. R. CIV. P. 20(a)(2)(B); *see also Disparte*, 223 F.R.D. at 11. The plaintiff has met this requirement as well. The plaintiff must establish against each putative defendant the same legal claims concerning the validity of the copyrights at issue and the infringement of the exclusive rights reserved to the plaintiff as the copyright holder. Furthermore, the putative defendants are alleged to have utilized the same BitTorrent file-sharing protocol to illegally distribute and download the plaintiff’s movies and, consequently, factual issues related to how BitTorrent works and the methods used by the plaintiff to investigate, uncover and collect evidence about the infringing activity will be essentially identical for each putative defendant. *See* Second Am. Compl., ¶ 3. The Court recognizes that each putative defendant may later present different factual and substantive legal defenses, but that does not defeat, at this stage of the proceedings, the commonality in facts and legal claims that support joinder under Rule 20(a)(2)(B).

In addition to the two requirements for permissive joinder under Rule 20(a)(2), the Court

must also assess whether joinder would prejudice the parties or result in needless delay. *See Lane*, 2007 WL 2007493, at *7; *M.K. v. Tenet*, 216 F.R.D. 133, 138 (D.D.C. 2002). At this stage in the litigation, it will not. The putative defendants are currently identified only by their IP addresses and are not named parties. They are thus not required to respond to the plaintiff's allegations or assert a defense. The putative defendants may be able to demonstrate prejudice should the plaintiff name and proceed with a case against them, but they cannot demonstrate any harm that is occurring to them before that time. In addition, rather than result in needless delay, joinder of the putative defendants facilitates jurisdictional discovery and expedites the process of obtaining identifying information, which is prerequisite to reaching the merits of plaintiff's claims. The Court therefore concludes that at this procedural juncture, the plaintiff has met the requirements of permissive joinder under Rule 20(a)(2) and joinder of the putative defendants is proper.¹⁹

This Court reaches this conclusion cognizant of the significant burdens on the court and judicial economy posed by the sheer number of putative defendants that the plaintiff seeks to join in a single lawsuit. These concerns are legitimately shared by other courts across the country that are confronting copyright infringement cases involving allegations of illegal file-sharing of copyrighted works by unprecedented numbers of Doe defendants, and the multitude of motions from interested parties that such suits engender. *Lightspeed*, 2011 U.S. Dist. LEXIS 35392, at *7 ("given the number of 'potential' defendants (i.e., Does 1-1000), [the] court could be faced with hundreds of factually unique motions to dismiss, quash or sever from potential defendants

¹⁹ For a more expansive discussion regarding the propriety of joining the putative defendants in this case, see the Court's Memorandum Opinion filed March 22, 2011 addressing amici Electronic Frontier Foundation, Public Citizen, American Civil Liberties Union Foundation, American Civil Liberties Union of the Nation's Capital's contention that joinder of the putative defendants is inappropriate in this case. *Call of the Wild Movie, LLC v. Does 1-1,062*, No. 10-cv-455, 2011 WL 996786 at *4-7 (D.D.C. Mar. 22, 2011) (consolidated opinion also addressing motions filed in *Maverick Entm't Grp., Inc. v. Does 2,115*, No. 10-cv-569).

located all over the country.”); *Millennium TGA Inc.*, 2011 U.S. Dist. LEXIS 35406, at *5 (same). Courts have varying thresholds for the exercise of their discretion to sever defendants in such cases. *See Bridgeport Music, Inc.*, 202 F.R.D. at 232-33 (even if joinder of over 700 named defendants was proper because claims arose from the same series of occurrences, “the Court would exercise the discretion afforded it to order a severance to avoid causing unreasonable prejudice and expense to Defendants and to avoid a great inconvenience to the administration of justice”).

This Court similarly must evaluate judicial economy and the administrative burdens of managing such cases, set against the challenge this broad-scale allegedly infringing activity also represents for the copyright owners. Copyright owners’ efforts to protect their copyrighted works through Doe actions are “costly[,] time consuming[,] . . . cumbersome and expensive.” *In re Charter Commc’ns, Inc., Subpoena Enforcement Matter*, 393 F.3d 771, 782 (8th Cir. 2005) (Murphy, J., dissenting). Yet, copyright owners have limited alternatives to obtain redress for infringement of their protected works other than such lawsuits. *See Arista Records LLC v. Does 1-27*, 584 F. Supp. 2d 240, 252 (D. Me. 2008) (“the Court begins with the premise that the Plaintiffs have a statutorily protected interest in their copyrighted material and that the Doe Defendants, at least by allegation, have deliberately infringed that interest without consent or payment. Under the law, the Plaintiffs are entitled to protect their copyrighted material and it is difficult to discern how else in this unique circumstance the Plaintiffs could act. Not to act would be to allow those who would take what is not theirs to remain hidden behind their ISPs and to diminish and even destroy the intrinsic value of the Plaintiffs’ legal interests.”); *In re Charter Commc’ns, Inc.*, 393 F.3d at 775 n.3 (“[A]s a practical matter, copyright owners cannot deter unlawful peer-to-peer file transfers unless they can learn the identities of persons engaged in that

activity.”). Courts must nonetheless maintain supervision of these lawsuits and, at some point, the sheer number of putative defendants involved in a single case may necessitate severance. At this stage of the litigation, with jurisdictional discovery well underway, the Court finds that judicial economy is best served by joinder of the putative defendants.

The putative defendants may raise the argument that they are improperly joined, under Federal Rule of Civil Procedure 20, and move to sever, under Federal Rule of Civil Procedure 21, after they have been identified and named in the Complaint. Severance prior to that point, as numerous other courts both in and outside this District have held, is premature. *See, e.g., Achte/Neunte Boll Kino Beteiligungs GMBH & Co, KG v. Does 1-4,577*, No. 10-cv-00453, ECF No. 34 (D.D.C. July 2, 2010) (Collyer, J.); *West Bay One, Inc. v. Does 1-1653*, No. 10-cv-00481, ECF No. 25 (D.D.C. July 2, 2010) (Collyer, J.); *Arista Records LLC v. Does 1-19*, 551 F. Supp. 2d 1, 11 (D.D.C. 2008) (Kollar-Kotelly, J.); *London-Sire Records, Inc. v. Doe 1*, 542 F. Supp. 2d 153, 161 n.7 (D. Mass. 2008); *Sony Music Entm’t, Inc. v. Does 1-40*, 326 F. Supp. 2d 556, 568 (S.D.N.Y. 2004).

V. MOTIONS TO DISMISS BASED ON LACK OF PERSONAL JURISDICTION

Forty-three putative defendants argue that they should be dismissed from the lawsuit because the Court lacks personal jurisdiction over them.²⁰ To support this argument, they supply

²⁰ *See* Cedric Johnson, ECF Nos. 14, 60 (IP address listed: 97.91.179.237); Lori Pearlman, ECF Nos. 34, 58 (IP address listed: 68.62.35.244); Xiangping Xu a.k.a. Kevin Xu, ECF No. 35, 56 (IP address listed: 67.170.234.17); Silvia R. Morgan, ECF No. 38 (No IP address listed); Theresa M. McNiff, ECF No. 39 (No IP address listed); Tyler Edwin Thomas, ECF No. 50 (No IP address listed); Granville Oral Barrett, ECF No. 51 (No IP address listed); Shedrika Power, ECF No. 52 (No IP address listed); Lian Oltean, ECF No. 53 (No IP address listed); Armando Liban, ECF No. 54 (No IP address listed); Nicholas Caruso, ECF No. 55 (No IP address listed); Brian Bunn, ECF No. 67 (No IP address listed); Robert Slade, ECF No. 68 (No IP address listed); Christian Murphy, ECF No. 69 (No IP address listed); Lucyna Kwasniak, ECF No. 76 (No IP address listed); Richard G. Scoza, ECF No. 78 (IP address listed: 69.249.32.138); Janice A. Harmis, ECF No. 79 (No IP address listed); Keith E. Nickoles, ECF No. 80 (No IP address listed); Raymond M. Duran, ECF No. 81 (No IP address listed); Marc Mordechai Mandel, ECF No. 82 (No IP address listed); Shelia A. Torrance, ECF No. 83 (No IP address listed); Daniel & Richard Probinsky, ECF No. 84 (No IP address listed); Antonio Forte, ECF No. 85 (No IP address listed); Mark Benavides, ECF No. 92 (IP address listed: 98.197.169.162); Felix Martinez, ECF No. 93 (No IP address listed); Linda White, ECF No. 94 (No IP address listed); Douglass Edward Oster, ECF No. 95 (No IP address listed); Victoria Kristian, ECF No. 102 (IP

affidavits or declarations attesting that they do not reside, transact or solicit business, or otherwise have sufficient contacts in the District of Columbia. These asserted facts would become relevant for the Court's consideration when and if these individuals are named as parties in this action. They cannot be dismissed, under Federal Rule of Civil Procedure 12(b)(2), from a lawsuit to which they are not parties.

Moreover, to establish personal jurisdiction, the Court must examine whether jurisdiction is applicable under the District of Columbia's long-arm statute, D.C. CODE § 13-423, and must also determine whether jurisdiction satisfies the requirements of due process. *See GTE New Media Servs. Inc. v. BellSouth Corp.*, 199 F.3d 1343, 1347 (D.C. Cir. 2000). Due Process requires the plaintiff to show that the defendant has "minimum contacts" with the forum, thereby ensuring that "the defendant's conduct and connection with the forum State are such that he should reasonably anticipate being haled into court there." *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286, 297 (1980); *see also GTE New Media Servs.*, 199 F.3d at 1347.

In cases where a party's contacts with the jurisdiction are unclear and the record before the court is "plainly inadequate," courts have allowed for a discovery period within which to gather evidence to support jurisdiction. *See GTE New Media Servs.*, 199 F.3d at 1351-52 (reversing lower court's finding of personal jurisdiction, but stating that "[t]his court has previously held that if a party demonstrates that it can supplement its jurisdictional allegations through discovery, then jurisdictional discovery is justified."). "This Circuit's standard for

address listed: 76.111.164.34); John Doe (IP address listed: 65.96.173.62) and John Doe (IP address listed: 24.128.252.215) represented by Tuna Mecit, Esq., ECF No. 103; Marie Sanchez, ECF No. 104 (IP address listed: 174.51.121.33); Jose Otero, ECF No. 105 (No IP address listed); Darrin Ross, ECF No. 108 (No IP address listed); Jane Doe represented by Emanuel J. Oakes, Jr., Esq., ECF No. 121, (IP address listed: 98.239.170.63); Jasmin Silva, ECF No. 123 (IP address listed: 24.6.177.153); Felicia Martin, ECF No. 125 (No IP address listed); Scott Cassel, ECF No. 126 (IP address listed: 67.161.196.74); Christopher C. Murdock, ECF No. 127 (No IP address listed); Cathy Patterson, ECF No. 128 (No IP address listed); Inna Shkrabak, ECF No. 129 (IP address listed: 24.18.48.58); Kamil Kierski, ECF Nos. 130, 132 (IP address listed: 98.217.10.245); Tom Ni, ECF No. 131 (IP address listed: 71.233.3.232).

permitting jurisdictional discovery is quite liberal,” *Diamond Chem. Co. v. Atofina Chems., Inc.*, 268 F. Supp. 2d 1, 15 (D.D.C. 2003), and jurisdictional discovery is available when a party has “at least a good faith belief” that it has personal jurisdiction. *Caribbean Broad. Sys., Ltd. v. Cable & Wireless PLC*, 148 F.3d 1080, 1090 (D.C. Cir. 1998). Courts have permitted discovery even when a party has failed to establish a *prima facie* case of personal jurisdiction. *See GTE New Media Servs.*, 199 F.3d at 1352 (“ . . . as the record now stands, there is absolutely no merit to [plaintiff]’s bold claim that the parent companies and subsidiaries involved in this lawsuit should be treated identically. Jurisdictional discovery will help to sort out these matters.”); *see also In re Vitamins Antitrust Litigation*, 94 F. Supp. 2d 26, 35 (D.D.C. 2000) (discussing *GTE New Media Servs.* and stating that “the D.C. Circuit held that although plaintiffs had failed to establish a *prima facie* case of personal jurisdiction and the court was unable to tell whether jurisdictional discovery would assist GTE on this score, plaintiffs were entitled to pursue [discovery].”). In such cases, a party is entitled to pursue “precisely focused discovery aimed at addressing matters relating to personal jurisdiction.” *GTE New Media Servs.*, 199 F.3d at 1352.

Although the putative defendants assert that they do not have sufficient contacts with this jurisdiction to justify personal jurisdiction, the Court, as well as the plaintiff, has limited information to assess whether these jurisdictional defenses are valid²¹ and to evaluate possible alternate bases to establish jurisdiction. *See, e.g., London-Sire Records, Inc.*, 542 F. Supp. 2d at

²¹ The putative defendants argue that the plaintiff should have used freely available tools that extract the geolocation information embedded in each IP address in order to verify the putative defendants’ location prior to filing claims in the District of Columbia. While it may behoove the plaintiff to utilize tools to ascertain the general location of the putative defendants prior to filing its case, these lookup tools are not completely accurate and it does not resolve for the Court the question of whether personal jurisdiction would be proper. Ultimately, the Court would still be unable to evaluate properly jurisdictional arguments until the putative defendants are identified and named. *See Sony*, 326 F. Supp. 2d at 567-68 (“Assuming personal jurisdiction were proper to consider at this juncture, the [publicly available IP lookup] techniques suggested by amici, at best, suggest the mere ‘likelihood’ that a number of defendants are located [outside this jurisdiction]. This, however, does not resolve whether personal jurisdiction would be proper.”).

181 (“Even taking all of the facts in [the putative defendant’s] affidavit as true, it is possible that the Court properly has personal jurisdiction.”); *Humane Soc’y of the United States v. Amazon.com, Inc.*, No. 07-623, 2007 U.S. Dist. LEXIS 31810, at *10 (D.D.C. May 1, 2007) (“[A] plaintiff faced with a motion to dismiss for lack of personal jurisdiction is entitled to reasonable discovery, lest the defendant defeat the jurisdiction of a federal court by withholding information on its contacts with the forum,” quoting *Virgin Records Am., Inc. v. Does 1-35*, No. 05-1918, 2006 WL 1028956, at *3 (D.D.C. Apr. 18, 2006)). To be clear, at this stage in the proceedings, the plaintiff is engaged in discovery to identify the proper defendants to be named in this lawsuit, including whether the exercise of jurisdiction over each potential defendant is proper. If and when the putative defendants are ultimately named in this lawsuit, the defendants will have the opportunity to file appropriate motions challenging the Court’s jurisdiction, and the Court will be able to evaluate personal jurisdiction defenses and consider dismissal. Until that time, however, dismissal under Rule 12(b)(2) is inappropriate.²² See *London-Sire Records*, 542 F. Supp. 2d at 180-181 (“premature to adjudicate personal jurisdiction” and permitting plaintiff to engage in jurisdictional discovery); *Sony*, 326 F. Supp. 2d. at 567-68 (same); *Virgin Records*, 2006 WL 1028956, at *3 (“Defendant’s Motion to Quash is without merit [] because it is premature to consider the question of personal jurisdiction in the context of a subpoena directed at determining the identity of the Defendant,” citing *Elektra Entm’t Grp., Inc. v. Does 1-9*, No. 04-2289, 2004 WL 2095581, at *5 (S.D.N.Y. Sept. 8, 2004); *UMG Recordings v. Does 1-199*, No. 04-0093, slip op. at 2 (D.D.C. Mar. 10, 2004)). Accordingly, the putative defendants’

²² A more expansive discussion regarding the personal jurisdiction issues involved in this case is contained in the Court’s Memorandum Opinion filed March 22, 2011, which addresses amici Electronic Frontier Foundation, Public Citizen, American Civil Liberties Union Foundation, American Civil Liberties Union of the Nation’s Capital’s contention that this case should be dismissed for lack of personal jurisdiction over the putative defendants. *Call of the Wild Movie, LLC v. Does 1-1,062*, No. 10-cv-455, 2011 WL 996786 at *7-10 (D.D.C. Mar. 22, 2011) (consolidated opinion also addressing motions filed in *Maverick Entm’t Grp., Inc. v. Does 2,115*, No. 10-cv-569).

motions to dismiss based on a purported lack of personal jurisdiction are denied at this time.

VI. CONCLUSION

For the reasons stated above, the putative defendants have failed to demonstrate that the plaintiff's subpoenas issued to ISPs should be quashed, that protective orders are warranted, or that the putative defendants should otherwise be dismissed from this case for improper joinder or a lack of personal jurisdiction. Accordingly, the following motions to quash the plaintiff's subpoenas, motions to be dismissed from the lawsuit, and motions for protective orders are denied: Robert A. Foster, ECF No. 12 (No IP address listed); Cedric Johnson, ECF Nos. 14, 60 (IP address listed: 97.91.179.237); Cindy Tate, ECF No. 20 (IP address listed: 68.187.201.11); Gundie Logan, ECF No. 20 (No IP address listed); Jose M. Barroso, ECF No. 20 (No IP address listed); Jane Doe, ECF No. 20 (IP address listed: 75.129.147.167); John Doe, ECF No. 20 (IP address listed: 68.191.210.134); Marty Ingebretsen, ECF No. 20 (IP address listed: 75.135.157.00); Maria Guadalupe Reyes, ECF No. 36 (IP address listed: 97.115.137.209); Juanita Burger, ECF No. 37 (No IP address listed); Silvia R. Morgan, ECF No. 38 (No IP address listed); Theresa M. McNiff, ECF No. 39 (No IP address listed); Tyler Edwin Thomas, ECF No. 50 (No IP address listed); Granville Oral Barrett, ECF No. 51 (No IP address listed); Shedrika Power, ECF No. 52 (No IP address listed); Lian Oltean, ECF No. 53 (No IP address listed); Armando Liban, ECF No. 54 (No IP address listed); Nicholas Caruso, ECF No. 55 (No IP address listed); Xiangping Xu a.k.a. Kevin Xu, ECF No. 56 (IP address listed: 67.170.234.17); Lori Pearlman, ECF No. 58 (IP address listed: 68.62.35.244); Connie Atkinson, ECF No. 62 (No

IP address listed); Jimmy Santana, ECF No. 63 (No IP address listed); Rohan Green, ECF No. 64 (No IP address listed); Robert McGrath, ECF No. 65 (No IP address listed); Sanjay Patel, ECF No. 66 (IP address listed: 69.254.240.39); Brian Bunn, ECF No. 67 (No IP address listed); Robert Slade, ECF No. 68 (No IP address listed); Christian Murphy, ECF No. 69 (No IP address listed); Lucyna Kwasniak, ECF No. 76 (No IP address listed); John Feher, ECF No. 77 (No IP address listed); Richard G. Scoza, ECF No. 78 (IP address listed: 69.249.32.138); Janice A. Harmis, ECF No. 79 (No IP address listed); Keith E. Nickoles, ECF No. 80 (No IP address listed); Raymond M. Duran, ECF No. 81 (No IP address listed); Marc Mordechai Mandel, ECF No. 82 (No IP address listed); Shelia A. Torrance, ECF No. 83 (No IP address listed); Daniel & Richard Probinsky, ECF No. 84 (No IP address listed); Antonio Forte, ECF No. 85 (No IP address listed); Phillip Bournes, ECF No. 89 (No IP address listed); Elizabeth Herrmann, ECF No. 90 (IP address listed: 71.226.65.201); Belton B. Raines, Jr., ECF No. 91 (No IP address listed); Mark Benavides, ECF No. 92 (IP address listed: 98.197.169.162); Felix Martinez, ECF No. 93 (No IP address listed); Linda White, ECF No. 94 (No IP address listed); Douglass Edward Oster, ECF No. 95 (No IP address listed); Victoria Kristian, ECF No. 102 (IP address listed: 76.111.164.34); John Doe (IP address listed: 65.96.173.62) and John Doe (IP address listed: 24.128.252.215) represented by Tuna Mecit, Esq., ECF No. 103; Marie Sanchez, ECF No. 104 (IP address listed: 174.51.121.33); Jose Otero, ECF No. 105 (No IP address listed); Dana Wilkerson, ECF No. 106 (IP address listed: 69.136.194); Tonya R. Moody, ECF No. 107 (General Motions to Dismiss; No IP address listed); Darrin Ross, ECF No. 108 (No IP address listed); Mary Woods, ECF No. 109 (IP address listed: 75.137.118.90); Eric Peterkin, ECF No. 119 (No IP address listed); Dianne J. Ashley, ECF No. 120 (IP address listed: 76.22.80.133); Jane Doe represented by Emanuel J. Oakes, Jr., Esq., ECF No. 121, (IP address listed:

98.239.170.63); Jasmin Silva, ECF No. 123 (IP address listed: 24.6.177.153); Felicia Martin, ECF No. 125 (No IP address listed); Scott Cassel, ECF No. 126 (IP address listed: 67.161.196.74); Christopher C. Murdock, ECF No. 127 (No IP address listed); Cathy Patterson, ECF No. 128 (No IP address listed); Inna Shkrabak, ECF No. 129 (IP address listed: 24.18.48.58); Kamil Kierski, ECF Nos. 130, 132 (IP address listed: 98.217.10.245); Tom Ni, ECF No. 131 (IP address listed: 71.233.3.232). An Order consistent with this Memorandum Opinion will be entered.

DATE: MAY 12, 2011

/s/ *Beryl A. Howell*
BERYL A. HOWELL
United States District Judge

Exhibit 15

to

Plaintiff's Response to Order to Show Cause - CV 10-04472 BZ

On The Cheap, LLC DBA Tru Filth, LLC v. Does 1-5011, Case No. CV 10-04472 BZ

United States District Court, Northern District of Illinois

Name of Assigned Judge or Magistrate Judge	Virginia M. Kendall	Sitting Judge if Other than Assigned Judge	
CASE NUMBER	10 C 6677	DATE	6/9/2011
CASE TITLE	MGCIP vs. Does 1 - 316		

DOCKET ENTRY TEXT

For the reasons stated, the Court denies the motions [101], [110], [115], [117], [118], [119], [121], [122], [123], [131], [132], set forth by a series of putative defendants. The Court finds that MCGIP's subpoena requests to internet service providers do not impose an undue burden on the putative defendants or require the disclosure of privileged matter. The Court also finds that the issue of personal jurisdiction is premature at this stage of the litigation because the putative defendants are not named defendants.

■ [For further details see text below.]

Docketing to mail notices.

00:04

STATEMENT

Plaintiff MCGIP, LLC ("MCGIP") filed suit against putative defendants John Does 1-316 alleging copyright infringement through the use of the BitTorrent protocol. A series of putative defendants have filed motions to quash subpoenas and motions to dismiss for lack of personal jurisdiction. *See, e.g.*, Docs. 110, 117, 118, 119, 121, 122, 132, 125. These putative defendants allege that the subpoenas improperly require the disclosure of privileged or protected matter and that the subpoenas impose an undue burden. These putative defendants also claim that this Court lacks personal jurisdiction over them because the putative defendants do not have a contractual relationship with an in-state party. For the following reasons, the Court denies the motions.

A court must quash or modify a subpoena that, in relevant part, "requires disclosure of privileged or other protected matter, if no exception or waiver applies; or subjects a person to undue burden." Fed. R. Civ. P. 45(c)(3). A general denial of engaging in copyright infringement, however, is not a basis for quashing a subpoena. *See, e.g., MCGIP, LLC v. Does 1-18*, 2011 WL 2181620 at *1 (N.D. Cal. June 2, 2011) (Chen, J.) (denying defendant's motion to quash subpoena); *Donkeyball Movie, LLC v. Does 1-171*, --- F.Supp.2d ---, 2011 WL 1807452 at *2 (D.D.C. May 12, 2011) (Howell, J.) ("The putative defendant's general denial that she engaged in copyright infringement is not a basis for quashing the plaintiff's subpoena.").

Here, the putative defendants cannot demonstrate an undue burden. MCGIP issued the subpoenas to internet service providers, not to the putative defendants. As such, the putative defendants cannot maintain that the subpoenas create an undue burden on them. *See, e.g., Donkeyball*, --- F.Supp.2d ---, 2011 WL 1807452 at *2 (finding that putative defendants "face no obligation to produce any information under the subpoena issued to [an internet service provider] and cannot claim any hardship, let alone undue hardship.").

STATEMENT

Nor can the putative defendants demonstrate that the subpoenas require disclosure of privileged matter. To the extent that they assert that MCGIP's subpoenas violate their First Amendment rights to anonymous speech and privacy, those assertions are unavailing. *See, e.g., Sony Music Entm't Inc. v. Does 1-40*, 326 F.Supp.2d 556, 567 (S.D.N.Y. 2004) (“[D]efendants’ First Amendment right to remain anonymous must give way to plaintiffs’ right to use the judicial process to pursue what appear to be meritorious copyright infringement claims.”). The First Amendment does not provide a license for copyright infringement and, as such, the putative defendants cannot rely on these arguments to prevent MCGIP from issuing subpoenas. *See Arista Records LLC v. Doe 3*, 604 F.3d 110, 118 (2d Cir. 2010); *see, e.g., Call of the Wild Movie, LLC v. Does 1-1,062*, --- F.Supp.2d ---, 2011 WL 996786 at *12 (D.D.C. Mar. 22, 2011) (Howell, J.) (noting that “a file-sharer’s First Amendment right to anonymity is ‘exceedingly small.’”) (collecting cases).

At this stage of the proceedings, MCGIP is merely seeking to identify who the defendants are based on their IP addresses. The Court finds that the subpoenas issued to that end do not require the disclosure of privileged matter or create an undue burden on the putative defendants. Nor are the subpoena requests outweighed by the putative defendants’s privacy interests or First Amendment rights. *See, e.g., MCGIP*, 2011 WL 2181620 at *1 (“[W]hile the Court is not unsympathetic to [the putative defendants’s] privacy argument, it is difficult to say that [the putative defendants] had a strong expectation of privacy because he or she either opened his or her computer to others through file sharing or allowed another person to do so.”). Therefore, the Court denies the putative defendants’s motions to quash MCGIP’s subpoenas.

The Court also finds that the putative defendants’s arguments that they were improperly joined are premature. *See Donkeyball*, --- F.Supp.2d ---, 2011 WL 1807452 at *4 (“At this stage in the litigation . . . when discovery is underway to learn identifying facts necessary to permit service on Doe defendants, joinder, under Federal Rule of Civil Procedure 20(a)(2), of unknown parties identified only by IP addresses is proper.”). The putative defendants may re-raise the issue of improper joinder should they become named defendants in this case. *See MCGIP*, 2011 WL 2181620 at *1 (“Doe’s assertion of improper joinder may be meritorious but, at this stage in the litigation, when discovery is underway only to learn identifying facts necessary to permit service on Doe defendants, joinder of unknown parties identified by IP addresses is proper.”) (quotations and citation omitted).¹¹ While a court in this district has granted a motion to sever regarding a copyright infringement case alleging the use of a BitTorrent protocol, it did so after finding that the claims against the putative defendants did not arise out of the same transaction or occurrence. *See, e.g., Lightspeed v. Does 1-1000*, 2011 LEXIS 35392 at *4 (N.D. Ill. Mar. 31, 2011) (Manning, J.) (sua sponte concluding that the putative defendants were improperly joined). Here, however, given the decentralized nature of BitTorrent’s file-sharing protocol—where individual users distribute the same work’s data directly to one another without going through a central server—the Court finds that sufficient facts have been plead to support the joinder of the putative defendants at this time. *See, e.g., Donkeyball*, --- F.Supp.2d ---, 2011 WL 1807452 at *8 (finding joinder proper and collecting cases holding that severance prior to the naming of the actual defendants was premature).

Similarly, the putative defendants’s motions to dismiss for lack of personal jurisdiction are also premature at this stage of the litigation. The Court reiterates that the putative defendants are not yet named defendants in the case. Moreover, the putative defendants, should they become named defendants in the case, will have the opportunity to contest this Court’s jurisdiction at that time. *See, e.g., Call of the Wild Movie, LLC v. Smith*, --- F.Supp.2d ---, 2011 WL 1807416 at *10 (D.D.C. May 12, 2011) (Howell, J.) (denying putative defendants’s motions to dismiss because the court only had limited information to determine whether the jurisdictional defenses were valid) (collecting cases); *London-Sire Records, Inc. v. Doe 1*, 542 F.Supp.2d 153, 180-81 (D. Mass. 2008) (finding it premature to adjudicate jurisdiction because the putative defendant’s affidavit—signed as a Doe defendant—was insufficient to determine the issue of jurisdiction given, for example, the state’s long-arm statute). Therefore, the Court denies the putative defendants’s motions to dismiss for lack of jurisdiction as premature.

STATEMENT

For the reasons stated, the Court denies the motions set forth by a series of putative defendants. The Court finds that MCGIP's subpoena requests to internet service providers do not impose an undue burden on the putative defendants or require the disclosure of privileged matter. The Court also finds that the issue of personal jurisdiction is premature at this stage of the litigation because the putative defendants are not named defendants.

PROOF OF SERVICE

I, Ira M. Siegel, hereby certify that I am a resident of the County of Los Angeles in California; I am over the age of eighteen years and am not a party to the within entitled action; and my business address is 433 N. Camden Drive, Suite 970, Beverly Hills, California 90210. I served a redacted version of the foregoing

**PLAINTIFF'S OPPOSITION TO MOTION TO
QUASH BY PUTATIVE DEFENDANT DOE 703**

on the interested parties in said action by placing a true copy thereof in sealed envelopes addressed as follows:

Putative defendant Doe 703
NONE-This movant provided no address whatsoever.

Putative defendant Doe M:
NONE-This putative defendant has withdrawn his, her or its appearance.

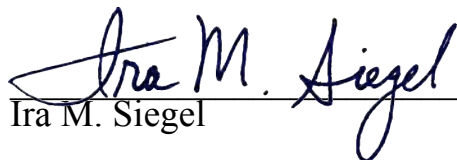
Putative defendant Doe T:
At the address in Doe T's papers.

Doe 406:
c/o
Custodian of Records Verizon Internet Services
Legal Compliance
P.O. Box 1001, TXD01316
San Antonio, TX 76902

and depositing each such envelope with United States priority mail postage thereon fully prepaid in the United States mail at a facility regularly maintained by the United States Postal Service at Los Angeles, California.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 13th day of July, 2011 at Los Angeles, California.


Ira M. Siegel